BEZPIECZEŃSTWO SEKTORA BANKOWEGO W OBLICZU WZROSTU RYZYKA GEOPOLITYCZNEGO

SYGN. PAB/WIB 13/2026

ISBN 978-83-910226-4-1

Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Warszawa, maj 2026

PROGRAM ANALITYCZNO BADAWCZY

O raporcie

Raport „Bezpieczeństwo sektora bankowego w obliczu wzrostu ryzyka geopolitycznego” został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości.

Autorzy

Raport przygotowany przez zespół w składzie:

Dr hab. Paweł Marszałek

Profesor Uniwersytetu Ekonomicznego w Poznaniu, Przewodniczący Rady Awanów Naukowych UEP oraz kierownik Katedry Pieniądza i Bankowości. Specjalizuje się w teorii pieniądza, polityce gospodarczej i historii myśli ekonomicznej, a także zajmuje się problematyką systemów bankowych i finansjalizacji. Autor ponad stu publikacji naukowych, w tym monografii „Systemy pieniężne wolnej bankowości. Koncepcje, cechy, zastosowanie”, nagrodzonej w 2016 roku w II edycji Konkursu o Nagrodę Prezesa NBP za wybitne publikacje książkowe z dziedziny bankowości i finansów. Pełnił m.in. funkcję doradcy Generalnego Inspektora Nadzoru Bankowego, Prodziekana Wydziału Ekonomii UEP, Dyrektora studiów zakresie finansów i rynków finansowych oraz Głównego Redaktora Wydawnictw Poznańskiego Towarzystwa Przyjaciół Nauk.

Prof. dr hab. Katarzyna Szarzec

Pracownik Uniwersytetu Ekonomicznego w Poznaniu, kierownik Katedry Makroekonomii i Badań nad Rozwojem, wiceprzewodnicząca Komitetu Nauk Ekonomicznych PAN. Specjalizuje się w makroekonomii i historii myśli ekonomicznej, a także zajmuje się rolą państwa w gospodarce. Autorka ponad stu publikacji naukowych, w tym monografii pt.: „Państwo w gospodarce: studium teoretyczne – od Adama Smitha do współczesności” i „Państwo jako właściciel przedsiębiorstw: polityka, gospodarka, dziedzictwo historyczne”. Pełniła m.in. funkcję Dyrektora Szkoły Doktorskiej UEP.

Dr Bartosz Totleben

Adiunkt w Katedrze Makroekonomii i Badań nad Rozwojem Uniwersytetu Ekonomicznego w Poznaniu. Jego zainteresowania badawcze obejmują analizę roli instytucji państwa w procesach wzrostu i rozwoju gospodarczego, w tym zagadnienia zawodności państwa oraz pogoni za rentą. Jest autorem kilkudziesięciu publikacji naukowych oraz kierownikiem i wykonawcą projektów badawczych finansowanych przez Narodowe Centrum Nauki.

Dr Daniel Wilusz

Adiunkt w Katedrze Technologii Informacyjnych Uniwersytetu Ekonomicznego w Poznaniu. Obszar jego zainteresowań badawczych obejmuje zagadnienia cyberbezpieczeństwa, zastosowań kryptografii, mechanizmów kontroli dostępu w systemach rozproszonych oraz funkcjonowania systemów elektronicznych płatności, ze szczególnym uwzględnieniem bezpieczeństwa cyfrowych usług płatniczych i ubezpieczeniowych. Posiada doświadczenie w projektach badawczych i technologicznych z zakresu bezpieczeństwa usług cyfrowych, w szczególności dotyczących płatności elektronicznych, ubezpieczeń kryptoaktywów oraz bezpiecznej komunikacji. Jego dorobek obejmuje m.in. prace nad pikopłatnościami strumieniowymi i anonimowymi mikropłatnościami, rozwiązaniami ubezpieczeniowymi dla kryptoaktywów wykorzystującymi mechanizmy kryptograficzne i inteligentne kontrakty, a także systemami bezpiecznej wymiany danych. Uczestniczy w międzynarodowych komitetach programowych i organizacyjnych konferencji naukowych oraz angażuje się w inicjatywy związane z cyfryzacją usług i rozwojem mikropoświadczeń.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wy korzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze
- Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego
- Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich
- ESG i sustainable finance
- Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

dr Radosław Ciukaj
m: 784 680 685
e: radoslaw.ciukaj@zbp.pl

Spis treści

Streszczenie kierownicze

Celem raportu jest **charakterystyka zjawiska ryzyka geopolitycznego i rozważenie w tym kontekście poziomu bezpieczeństwa sektora bankowego w Polsce**. Szczególną uwagę zwrócono na źródła ryzyka geopolitycznego (ze szczególnym uwzględnieniem tzw. cyberzagrożeń), jego rodzaje, mechanizmy (kanały) wpływu na instytucje bankowe, konsekwencje oraz sposoby zarządzania tym ryzykiem. Sformułowane zostaną także rekomendacje dla polskich instytucji bankowych i decydentów odnośnie do strategii i działań względem ryzyka geopolitycznego.

Raport składa się z czterech części. W pierwszej z nich opisano teoretyczne kwestie dotyczące geopolityki i ryzyka geopolitycznego. W części drugiej przedstawiono wybrane manifestacje ryzyka geopolitycznego w sferze monetarnej i finansowej: cyberzagrożenia dla sektora finansowego, konsekwencje tego ryzyka dla rynku kryptowalut, przepływy kapitałowe i bezpośrednie inwestycje zagraniczne oraz kwestie funkcjonowania sfery gotówkowej i ryzyka odpływu depozytów. Część trzecia dotyczy już *stricte* ryzyka geopolitycznego w działalności banków – mechanizmów, konsekwencji i sposobów ograniczania w systemach bankowych. Przedmiotem rozważań w części czwartej jest natomiast polski system bankowy w kontekście ryzyka geopolitycznego. Przybliżono występowanie i nasilenie tego ryzyka w Polsce, swoiste cechy polskiego systemu bankowego w kontekście ryzyka geopolitycznego, a także wybrane wyzwania stojące przed krajowym systemem bankowym w kontekście ryzyka geopolitycznego.

W końcowej części przedstawiono rekomendacje w zakresie ograniczania tego ryzyka i skutków jego wystąpienia. Natomiast w aneksie scharakteryzowano – pod kątem potencjalnych stress-testów – możliwe scenariusze manifestacji ryzyka geopolitycznego i ich następstw.

1. Jednym z elementów typowej dla ostatnich lat rosnącej złożoności i kruchości warunków funkcjonowania całych gospodarek, poszczególnych rynków i branż, jak i pojedynczych instytucji czy podmiotów jest prymat (geo) polityki nad gospodarką. Wiąże się z tym dramatyczny wzrost tzw. **ryzyka geopolitycznego**. Zjawisko to, najogólniej rozumiane jako ryzyko związane z napięciami wpływającymi na normalny i pokojowy przebieg stosunków międzynarodowych (np. ataki terrorystyczne, cyberataki, konflikty kinetyczne i gospodarcze, problemy z łańcuchami dostaw, kryzysy energetyczne i migracyjne), jest czynnikiem coraz silniej wpływającym także na instytucje i rynki finansowe poszczególnych krajów. W zglobalizowanym świecie, w którym współzależności międzynarodowe urosły do nieznanych wcześniej rozmiarów, **ryzyko geopolityczne staje się kluczowym czynnikiem, który należy brać pod uwagę**.

2. Mimo swojego znaczenia, źródła, mechanizmy i kanały oddziaływania ryzyka geopolitycznego oraz konsekwencje, jakie ma ono – i może mieć – dla sektora bankowego **nadal nie są dokładnie rozpoznane**. Utrudnia to zaprojektowanie właściwych rozwiązań, mających ograniczyć to ryzyko oraz zapobiec negatywnym skutkom, jakie jego realizacja miałaby dla instytucji bankowych. Kwestia jest o tyle skomplikowana, że ryzyko geopolityczne z samej swojej natury **jest czynnikiem egzogenicznym dla banków** (być może z pewnymi wyjątkami w odniesieniu do największych instytucji globalnych); mogą one w odniesieniu do tego ryzyka przybierać raczej postawy głównie reaktywne.

3. Wśród najważniejszych punktów bieżącej agendy geopolitycznej można wskazać następujące elementy:
   - **Geografia i zasoby** – przebieg i bezpieczeństwo szlaków handlowych, dostęp do mórz, rozmieszczenie surowców naturalnych (ropa, gaz, minerały, metale ziem rzadkich), dostępność wody i żywności, kwestie klimatyczne.
   - **Strefy wpływów i rywalizacja państw** – konkurencja między wielkimi mocarstwami/blokami (USA, Chiny, Indie, Rosja, UE) o dominację w kluczowych regionach (Pacyfik, Europa Wschodnia, Bliski Wschód, Afryka).
   - **Szlaki handlowe i komunikacyjne** – kontrola nad cieśninami morskimi, kanałami, rurociągami i szlakami transportowymi (m.in. takie inicjatywy jak Nowy Jedwabny Szlak, Północna Droga Morska); potencjalna ekonomiczna eksploracja (bliskiego) kosmosu.
   - **„Rywalizacja" ustrojowa** – relacje między kapitalizmem finansowym a kapitalizmem przemysłowym; demokracja (liberalna) vs autorytaryzm.

- **Bezpieczeństwo energetyczne** – zależności energetyczne, dywersyfikacja dostaw, transformacja energetyczna i jej wpływ na równowagę sił.
- **Technologia i cyberprzestrzeń** – kontrola nad infrastrukturą cyfrową, standardami technologicznymi (5G, AI), bezpieczeństwo cybernetyczne jako nowa arena rywalizacji; fragmentacja internetu; FinTech i systemy płatności.
- **Perspektywy przemian systemów pieniężnych i finansowych** – tendencje ku dedolaryzacji, kryptowaluty, neobankowość, poszukiwania nowej globalnej waluty rezerwowej.
- **„Wojny" walutowe i monetarne** – „weaponizacja" waluty, funkcjonowanie SWIFT i systemów konkurencyjnych; działania dewaluacyjne; sankcje finansowe; swoboda (lub brak) przepływów finansowych.
- **Reorientacja handlu światowego** – reshoring, nearshoring i friendshoring w miejsce offshoringu; proliferacja barier handlowych (ceł oraz instrumentów pozataryfowych).
- **Sojusze i instytucje międzynarodowe** – NATO, BRICS, SCO (Shanghai Cooperation Organization), UE; regionalne porozumienia: ich ewolucja i zmiana znaczenia w multipolarnym świecie; Północ vs Południe.
- **Konflikty i punkty zapalne** – Tajwan, Ukraina, Bliski Wschód, Morze Południowochińskie jako obszary potencjalnych eskalacji.

4. Obecne ryzyko geopolityczne jest bardziej złożone i trudniejsze do przewidzenia. Stawia to większe wymagania przed uczestnikami procesów politycznych i gry rynkowej oraz wymaga nowego podejścia do analizy oraz zarządzania bezpieczeństwem sektorowym i międzynarodowym. **Wyraźniejszy niż w okresie „klasycznej" geopolityki jest przy tym obecnie wymiar ekonomiczny napięć geopolitycznych**, a systemy finansowe, monetarne i płatnicze są płaszczyzną intensywnej rywalizacji. W warunkach natężenia i przyspieszenia procesów finansyzacji gospodarki i życia społecznego, typowych dla końca ubiegłego i początków tego stulecia, właśnie ten wymiar ryzyka geopolitycznego i czynniki z nim związane nabierają szczególnego znaczenia.

5. W odniesieniu do banków kanały, jakimi przenosi się ryzyko geopolityczne, są liczne i złożone, wiążąc się przy tym z samą istotą działalności oraz z innymi rodzajami ryzyka bankowego. Na ogólnym poziomie, można wyróżnić **cztery główne kanały przenoszenia szoków geopolitycznych na system bankowy**:

- **Kanał gospodarki realnej** – zmniejszenie produkcji na skutek zakłóceń w funkcjonowaniu łańcuchów dostaw i transakcji handlowych, skutkujące niedostępnością środków produkcji lub wzrostem ich cen. Rezultatem finalnym może być wolniejsze tempo wzrostu gospodarczego – także wskutek gorszych nastrojów konsumentów i producentów oraz trudniejszych warunków finansowania, zwłaszcza w krajach z wysokim lub rosnącym długiem publicznym. Niski wzrost gospodarczy lub recesja i/lub podwyższona inflacja będą negatywnie oddziaływać na kondycję gospodarstw domowych i przedsiębiorstw, a w konsekwencji pogarszać ich zdolność do obsługi zadłużenia i zwiększać ryzyko kredytowe.
- **Kanał powiązań finansowych** – zaburzenia strumieni finansowych w postaci kredytów i pożyczek, bezpośrednich inwestycji zagranicznych lub inwestycji portfelowych. W konsekwencji wystąpić mogą spadki wycen aktywów i nasilona zmienność stóp procentowych i kursów walutowych. Pogorszyć może się również wycena skarbowych papierów wartościowych utrzymywanych przez instytucje finansowe w portfelu handlowym, w szczególności w przypadku problemów z równowagą finansów publicznych (trudną do zapewnienia w warunkach konfliktów militarnych i konieczności sfinansowania zbrojeń).
- **Kanał podwyższonej niepewności** – występują tu dwa rodzaje zależności: w odniesieniu do niekorzystnych tendencji w sferze realnej oraz tych ze sfery finansowej. W tym pierwszym przypadku zaburzenia w gospodarce realnej powodują spadek nastrojów i zaufania gospodarstw domowych oraz przedsiębiorstw, co prowadzi do zmniejszenia wydatków konsumpcyjnych i inwestycyjnych. Dodatkowo osłabia to dynamikę wzrostu gospodarczego i zwiększa ryzyko kredytowe banków. W drugim przypadku niepewność dotycząca kategorii nominalnych, finansowych skutkuje wyższą zmiennością cen i wyższą awersją do ryzyka na rynkach finansowych. To zaś zwiększa koszt kredytu lub powoduje ograniczenie jego dostępności w wyniku trudności z oszacowaniem ryzyka kredytowego potencjalnych kredytobiorców lub odpływem kapitału w kierunku tzw. *safe havens*.
- **Kanał ryzyka operacyjnego** – konsekwencje skutecznych cyberataków na infrastrukturę krytyczną danego kraju, instytucje finansowe i ich systemy informatyczne lub dostawców ich kluczowych systemów informatycznych.

6. Najbardziej narażone na ryzyko geopolityczne wydają się być:

I. Banki z wysoką ekspozycją międzynarodową:
- banki z placówkami w regionach geopolitycznie niestabilnych;
- banki finansujące handel zagraniczny z krajami objętymi napięciami/sankcjami;
- banki z portfelami kredytowymi w walutach obcych, szczególnie z krajów „ryzykownych".

II. Banki o określonej strukturze własnościowej:
- banki będące własnością zagranicznych inwestorów, zwłaszcza z krajów objętych sankcjami;
- instytucje współpracujące z bankami państwowymi krajów autorytarnych;
- banki z udziałowcami powiązanymi z reżimami politycznymi.

III. Banki specjalizujące się w określonych segmentach, w szczególności:
- banki korporacyjne obsługujące międzynarodowe koncerny z wysoką ekspozycją na ryzyko geopolityczne;
- banki finansujące projekty infrastrukturalne w niestabilnych regionach;
- banki inwestycyjne aktywne na rynkach wschodzących.

IV. Banki o specyficznym profilu działalności, wrażliwym z punktu widzenia zależności geopolitycznych:
- banki silnie zaangażowane w finansowanie surowców energetycznych;
- banki obsługujące klientów z branż obronnych;
- banki obsługujące klientów branży technologicznej;
- banki-korespondenci instytucji z krajów wysokiego ryzyka.

V. Banki o dużym, z różnych względów, znaczeniu dla krajowego systemu:
- banki duże, ze złożoną strukturą operacji;
- banki ważne systemowo, będące z tego powodu obiektem szczególnej uwagi potencjalnych rywali;
- banki ważne ze względu na ich udział w aktywnościach i operacjach państwowych.

7. Konsekwencje ryzyka geopolitycznego dla banków można podzielić na sześć ogólnych grup: (1) konsekwencje dla działalności operacyjnej; (2) konsekwencje dla ryzyka kredytowego i jakości portfela; (3) konsekwencje w zakresie ryzyka rynkowego; (4) konsekwencje dla płynności; (5) kwestie regulacji i *compliance* oraz (6) pogorszenie sytuacji klientów.

8. Do **konsekwencji dotyczących działalności operacyjnej** zalicza się takie związane z ryzykiem geopolitycznym problemy jak: (1) zakłócenia w dostępie/użytkowaniu systemów płatniczych i infrastrukturze transgranicznej (szczególnie przy odcięciu od systemów typu SWIFT); (2) problemy z płynnością walutową i dostępem do finansowania w walutach rezerwowych; (3) skokowy wzrost kosztów zabezpieczeń cybernetycznych i ryzyka oraz konsekwencje ataków hybrydowych; (4) trudności z usługodawcami IT czy innymi kluczowymi dostawcami z regionów objętych konfliktami; (5) konieczność reorganizacji sieci placówek i operacji w strefach konfliktu lub sąsiadujących ze strefami konfliktu oraz (6) problemy z zapewnieniem kadry w obliczu eskalacji zagrożeń.

9. W odniesieniu do **ryzyka kredytowego i jakości portfela** realizacja ryzyka geopolitycznego oznacza pogorszenie obu kategorii: rośnie poziom ryzyka kredytowego, a jakość portfela pogarsza się – rośnie wolumen „złych" kredytów. Dotyczy to zwłaszcza pogorszenia zdolności (ale i wiarygodności) kredytowej klientów korporacyjnych, szczególnie narażonych na konflikty. Wzrost NPL (*non-performing loans*) następuje głównie w sektorach wrażliwych (handel międzynarodowy, łańcuchy dostaw, sektor energetyczny, wrażliwe technologie), ale wraz z przedłużaniem się sytuacji kryzysowych może on dotknąć również branże niepodatne wprost na ryzyko geopolityczne. Pojawiają się także problemy z zabezpieczeniami kredytów, a z czasem – także niemożliwość odzyskania należności

10. Negatywne następstwa w zakresie **ryzyka rynkowego** dla banków uwidaczniają się dość szybko, rzutując na podstawowe kategorie finansowe. Mianowicie, jako reakcja na szoki geopolityczne, pojawiają się gwałtowne wahania kursów walutowych, wpływając na pozycje walutowe banków, następują zmiany stóp procentowych, następuje przeszacowanie portfeli papierów wartościowych (szczególnie obligacji skarbowych), a także występują problemy z wyceną instrumentów pochodnych przy bardzo znaczącej ich zmienności.

11. Sytuację dodatkowo pogarsza wzrost **ryzyka płynności**, który w skrajnym przypadku może nawet przybrać formę runu na banki. Typowe i powszechne są też problemy z refinansowaniem na rynkach hurtowych, „zamrożenie" rynków międzybankowych i wspomniany ograniczony dostęp do walut obcych

12. Banki stają przed wyzwaniami związanymi z **kwestiami regulacji i compliance**. W warunkach rosnącego ryzyka geopolitycznego zachodzi bowiem konieczność szybkiej (czasem wręcz niemal natychmiastowej) implementacji sankcji międzynarodowych. Zbyt późne ich wprowadzenie czy też naruszenie sankcji może skutkować poważnymi konsekwencjami dla instytucji, która dopuściła się zaniedbań w tym obszarze. Tymczasem szybkie dostosowanie procedur generuje znaczące koszty i zwiększa ryzyko błędów. Innym problemem w tym zakresie może być konieczność dopasowania się do zwiększonych przez nadzorców wymogów kapitałowych, a także koszty związane z presją na *stress testing*, uwzględniający rozmaite niekorzystne scenariusze geopolityczne.

13. Czynnikiem, na który wpływają dotychczas charakteryzowane grupy konsekwencji ryzyka geopolitycznego, ale który ma także swoją własną specyfikę, jest **sytuacja klientów bankowych**. Są oni konfrontowani z rosnącą niepewnością, trudniejszym (lub po wyższym koszcie) dostępem do usług bankowych, w tym zwłaszcza tych związanych z aktywnością ponadnarodową.

14. Skutki wzrostu ryzyka geopolitycznego i/lub jego manifestacji mają **różny horyzont czasowy**. Niektóre z nich pojawiają się natychmiast (kwestia dni/tygodni), jak na przykład załamanie kursów walutowych, spadki cen akcji czy problemy z płynnością na rynkach międzynarodowych. Wystąpienie innych może zająć miesiące, np. pogorszenie jakości portfeli bankowych wskutek wzrostu stopy NPL w ekspozycjach bezpośrednich, spadek rentowności z tytułu ograniczeń działalności czy koszty dostosowania się do nowych regulacji/sankcji. Inne z kolei negatywy ujawniają w horyzoncie 1–3 lat, przybierając formę trwałego wzrostu kosztów ryzyka, konieczności restrukturyzacji modeli biznesowych czy dokonania odpisów z tytułu utraconych aktywów. Wreszcie, ostatecznie pojawią się skutki długofalowe (powyżej 3 lub nawet 5 lat), w postaci zmian geografii działalności danego banku, przekształcenia łańcuchów dostaw finansowych czy wreszcie nowych regulacji międzynarodowych.

15. Ryzyko geopolityczne powoduje zaostrzenie problemów w zasadzie w każdym z obszarów „tradycyjnych" rodzajów ryzyka bankowego, stanowiąc swoiste „metaryzyko". Nie będąc odrębną kategorią w klasycznym podziale głównych ryzyk bankowych (kredytowych, rynkowych, operacyjnych, płynności), działa jako czynnik egzogeniczny, swoisty katalizator, który intensyfikuje wszystkie pozostałe kategorie ryzyka.

16. Ryzyko geopolityczne można ograniczać na wiele sposobów, skupiając uwagę na rozmaitych płaszczyznach. W szczególności, można tu wskazać następujące obszary działań:

- aspekty ponadnarodowe (organizacje i porozumienia międzynarodowe);
- aspekty makroekonomiczne (polityka makroekonomiczna, polityka energetyczna, itp.);
- aspekty regulacyjne i nadzorcze;
- aspekty sektorowe, związane z działalnością operacyjną samych banków;
- aspekty technologiczne (cyberbezpieczeństwo, zabezpieczenia, systemy rozproszone, itp.).

17. Polska, z uwagi głównie na uwarunkowania historyczne, jest raczej „biorcą", niż generatorem ryzyka tego typu. Ryzyko geopolityczne jest dla naszej gospodarki i składających się na nią podmiotów (w tym banków) zmienną egzogeniczną.

18. Ostatnie lata przyniosły **znaczący wzrost ryzyka geopolitycznego dla Polski**, a tym samym – także dla polskiego systemu bankowego. Wśród najważniejszych źródeł tego ryzyka można wymienić przede wszystkim:

- **Konflikt w Ukrainie i bezpieczeństwo regionalne.** Wojna w Ukrainie pozostaje największym bezpośrednim zagrożeniem. Może wpłynąć na stabilność finansową regionu, wywołać dalsze fale uchodźców generujące koszty społeczne oraz prowadzić do zwiększonych wydatków obronnych obciążających budżet państwa. Niewykluczona jest także dalsza eskalacja konfliktu, która może dodatkowo zakłócić handel, łańcuchy dostaw, a także rozszerzyć się o działania poniżej progu wojny kinetycznej, ale mające już znamiona wojny hybrydowej (np. atak rosyjskich dronów w nocy z 9 na 10 września 2025 r., sytuacja na granicy białoruskiej).

- **Relacje z Rosją i sankcje.** Przedłużające się sankcje wobec Rosji wpływają na polskie banki przez ograniczenia w handlu i inwestycjach. Istnieje ryzyko dalszego zaostrzenia sankcji lub rosyjskich działań odwetowych, które mogą dotknąć polskich instytucji finansowych mających jeszcze jakiekolwiek powiązania z rynkiem rosyjskim (oraz białoruskim).
- **Zmiany w polityce UE i strefie euro.** Zmiany w polityce fiskalnej i monetarnej UE (zmiany celów, instrumentów, zasad funkcjonowania), a także perspektywa potencjalnej integracji polskiej gospodarki ze strefą euro mogą wpłynąć na polskie banki.
- **Relacje transatlantyckie.** Zmiany w polityce USA wobec Europy Środkowej mogą wpłynąć na przepływy kapitału i inwestycje amerykańskie w polskim sektorze bankowym. Polityka handlowa USA również może oddziaływać na polską gospodarkę, zarówno samą w sobie, jak i część UE.
- **Napięcia z Chinami.** Rosnące napięcia geopolityczne między Zachodem a Chinami mogą wpłynąć na gospodarcze relacje między Polską a Państwem Środka; polskie banki obsługujące handel z Azją mogą natrafić na mniej sprzyjające warunki, ograniczeniu może też ulec dostęp do chińskich inwestycji i technologii.
- **Ryzyko cybernetyczne.** Zwiększone zagrożenia cybernetyczne ze strony państw wrogich, szczególnie w kontekście konfliktu w Ukrainie, stanowią poważne ryzyko dla infrastruktury bankowej.
- **Konflikty w innych częściach świata.** Rosnące napięcia w wielu regionach świata (Iran, Izrael, Pakistan) zmieniają ceny importowanych przez Polskę surowców, oddziałują na ogólną niestabilność i stopień zaangażowania głównych podmiotów.

19. W kontekście tak poważnych i zróżnicowanych zagrożeń dla stabilności i rozwoju państwa polskiego i polskiej gospodarki pojawia się pytanie, na ile polski system bankowy jest podatny na poszczególne formy ryzyka geopolitycznego, a na ile dysponuje cechami oraz mechanizmami obronnymi, chroniącymi go przed materializacją ryzyka geopolitycznego wraz z wszystkimi opisanymi negatywnymi następstwami

20. Jeżeli chodzi o strukturę własnościową polskiego systemu bankowego oraz jej implikacje geopolityczne, należy wskazać w pierwszej kolejności na **wysoki udział kapitału zagranicznego**. Czynnik taki zasadniczo postrzega się jako zwiększający podatność danego systemu bankowego na to ryzyko, ale ważnym, by nie rzec kluczowym, czynnikiem jest tu struktura tego kapitału – ryzyko geopolityczne jest wyższe, jeżeli udziałowcy (właściciele) krajowych banków pochodzą z krajów rywalizujących, zaliczanych do przeciwstawnych obozów lub posiadających rozbieżne interesy geopolityczne. Nie jest to jednak przypadek Polski – **kapitał zagraniczny w polskim systemie bankowym pochodzi w zasadzie prawie w całości z krajów „sojuszniczych"** (głównie z UE), a przy tym jest rozproszony, co również ogranicza ryzyko geopolityczne związane z tym czynnikiem. Zaangażowanie kapitału zagranicznego nie tylko nie zwiększa zatem ryzyka geopolitycznego, ale wręcz je mityguje, albowiem ewentualny atak na Polskę uderza również w interesy tych banków i tych państw, które na naszym rynku funkcjonują.

21. Typowa dla polskiego rynku bankowego jest jego **segmentacja** – wyraźny jest podział na banki komercyjne, w których w ostatnich latach wzrosło znaczenie kapitału krajowego, przy zróżnicowanym geograficznie kapitale zagranicznym, oraz sektor spółdzielczy; specjalne miejsce w sektorze zajmują przy tym PKO BP – z uwagi na uwarunkowania historyczne, skalę działalności oraz silne powiązanie ze Skarbem Państwa – oraz BGK jako bank państwowy. Ta fragmentacja oznacza różną ekspozycję na poszczególne rodzaje ryzyka geopolitycznego.

22. W odniesieniu do specyfiki operacyjnej polskich banków można wskazać na ciągle obecny (choć zmniejszający się) **problem kredytów frankowych**; portfel kredytów walutowych (głównie CHF) w polskich bankach stanowi unikalną cechę, która czyni je wrażliwymi na gwałtowne wahania kursowe spowodowane napięciami geopolitycznymi. Ponadto polskie banki mają **stosunkowo wysoką ekspozycję kredytową na małe i średnie przedsiębiorstwa**, a więc podmioty, które są szczególnie wrażliwe na szoki energetyczne i problemy w funkcjonowaniu łańcuchów dostaw.

23. Jeżeli chodzi o koncentrację geograficzną, polskie banki **działają głównie na terytorium krajowym**; ich ekspansja zagraniczna (poza nielicznymi wyjątkami, jak działalność niektórych banków w regionie) zawsze była raczej znikoma. To oznacza całkowitą ekspozycję w zasadzie tylko na ryzyko krajowe bez dywersyfikacji geograficznej.

24. Za bardzo pozytywną cechę polskiej bankowości można uznać **wysoki poziom cyfryzacji**. Polskie banki są stosunkowo zaawansowane technologicznie (wysoki poziom bankowości mobilnej i internetowej). Należy jednak podkreślić, iż paradoksalnie zwiększa to ryzyko cyberataków – większa jest przestrzeń do tego typu działań. Ponadto wiele kluczowych systemów bankowych opiera się na rozwiązaniach zagranicznych dostawców, co tworzy potencjalną słabość w scenariuszu eskalacji napięć geopolitycznych (zob. Aneks). Cyfryzacja sprawia przy tym, że systematycznie maleje sieć fizycznych oddziałów i bankomatów, na co należy zwrócić uwagę, organizując zapewnienie podmiotom gospodarującym dostępu do gotówki.

25. Ramy instytucjonalne funkcjonowania polskich banków są **właściwie skonstruowane i funkcjonują skutecznie** na przestrzeni całego okresu po rozpoczęciu transformacji. Polska była krajem, w którym nie wystąpił kryzys bankowy, co niewątpliwie można zawdzięczać m.in. wysokiej jakości instytucji okołobankowych. Współcześnie, jak się wydaje, Komisja Nadzoru Finansowego prowadzi stosunkowo ostrożną i konserwatywną politykę nadzorczą, co z jednej strony buduje odporność sektora, ale z drugiej może ograniczać elastyczność w reagowaniu na szoki. Czynnikiem zwiększającym bezpieczeństwo jest także sukcesywna, kompleksowa implementacja regulacji unijnych. Polska specyfika polega przy tym na często nawet bardziej restrykcyjnej implementacji dyrektyw UE. Zwiększa to wprawdzie obciążenia **compliance**, ale tworzy jednocześnie dodatkowy bufor regulacyjny.

26. **Stosunkowo duża jest wrażliwość na politykę fiskalną i monetarną** (np. wakacje kredytowe, podatek bankowy i jego konstrukcja, wyższa stawka CIT dla banków – stawka 30% od 2026 r.); decyzje w zakresie policy mix mogą być podejmowane w reakcji na napięcia geopolityczne, tworząc dodatkowy kanał transmisji wpływu na system finansowy, co jednak może być czynnikiem raczej destabilizującym. Jak się wydaje, nadmierne i niekorzystne z punktu widzenia rozwoju banków i kształtowania się ich struktury bilansowej rozwiązania fiskalne, nastawione głównie na generowanie bieżących wpływów budżetowych, są działaniami generującymi dla decydentów korzyści doraźne, kosztem przyszłych. W dłuższej perspektywie presja fiskalna ogranicza rozwój instytucji bankowych, a tym samym niweluje korzyści, jakie większy i silniejszy kapitałowo system mógłby kreować dla sfery realnej. Dodatkowo tworzy ona trwałą nierównowagę, czy wręcz asymetrię rynkową, która w dłuższej perspektywie może obniżyć konkurencyjność sektora bankowego zarówno na poziomie krajowym, jak i międzynarodowym.

27. Typowy dla polskiego sektora bankowego jest **bardzo wysoki, dominujący udział depozytów** gospodarstw domowych w finansowaniu banków. W kontekście kanałów wpływu ryzyka geopolitycznego może to powodować podatność i wrażliwość na nastroje społeczne oraz potencjalnie zwiększać ryzyko paniki bankowej w scenariuszu kryzysu wywołanego napięciami geopolitycznymi (np. w warunkach sterowanej w ramach wojny hybrydowej kampanii czarnego PR czy dezinformacji). Z drugiej jednak strony, należy wskazać na pozytywną, zwiększającą stabilność systemu, rolę „osadu" depozytowego, typowego dla polskich banków. Ponadto, ważnym czynnikiem także wpływającym pozytywnie na stabilność depozytów jest ich duże rozdrobnienie podmiotowe oraz wysoki udział środków gwarantowanych – oba czynniki sprawiają, że depozyty są w mniejszym stopniu podatne na masowe odpływy.

28. Polski system bankowy pozostaje stabilny. Bardzo pozytywnie można ocenić zarówno spełnianie wymogów kapitałowych, jak i rentowność polskich banków (rekordowe zyski w 2024 roku albo latach 2024 i 2025). Bardzo niekorzystnym zjawiskiem jest natomiast istniejąca od stycznia 2025 r. sytuacja, w której polski sektor bankowy ma więcej instrumentów dłużnych (głównie Skarbu Państwa) niż kredytów, co jest ewenementem na skalę europejską i światową.

29. Pozycja polskiego systemu bankowego w kontekście ryzyka geopolitycznego **pozostaje dość specyficzna**. Polski sektor bankowy pozostaje jednym z mniejszych w UE (relacja kapitału własnego do PKB plasuje Polskę na przedostatnim miejscu w UE). Niemniej, jest on tzw. „małym gigantem", o znaczącej roli regionalnej i – mimo wszystko – istotnej pozycji strategicznej. Wynika to z kilku kwestii. **Po pierwsze**, jest on swoistą „bramą" do całego regionu Europy Środkowej i Wschodniej. Choć polski sektor jest stosunkowo mały w relacji do PKB, Polska jest największą gospodarką w regionie Europy Środkowo-Wschodniej. Ewentualna destabilizacja polskiego sektora bankowego mogłaby uruchomić efekt domina na cały region przez powiązania własnościowe, kanały handlowe i łańcuchy dostaw oraz względy psychologiczne. **Po drugie**, pojawia się kwestia finansowania bezpieczeństwa i obrony. Polska w ostatnich latach zwiększa wydatki obronne

(do 4% PKB), co wymaga bardzo dużego finansowania. Sektor bankowy pełni tu kluczową rolę w finansowaniu kontraktów zbrojeniowych, kredytowaniu przemysłu zbrojeniowego oraz obsłudze przepływów pieniężnych związanych z obecnością sił NATO. Destabilizacja sektora bezpośrednio uderzyłaby w zdolność Polski do umacniania swojej armii, a tym samym całej wschodniej flanki NATO. **Po trzecie**, polski system bankowy dominuje w regionie pod względem nowych technologii i rozwoju bankowości cyfrowej. Polskie rozwiązania (BLIK, infrastruktura cyfrowa) są eksportowane i kopiowane w regionie. W tej sytuacji, sukces cyberataku na polskie banki podważyłby zaufanie do cyfryzacji w całym regionie, spowolniłby adopcję innowacji finansowych, a także stworzyłby precedens i ułatwił cyberataki na inne kraje. **Po czwarte**, wskazana wada strukturalna, czyli przewaga w portfelach polskich banków instrumentów dłużnych zamiast kredytów, oprócz negatywnych następstw dla poszczególnych banków i zaopatrzenia gospodarki w środki finansowe, ma też znaczenie systemowe. Mianowicie, wzrost rentowności obligacji Skarbu Państwa mógłby w obecnej sytuacji spowodować destabilizację systemu bankowego, problemy z wartością złotego oraz konieczność zapobiegania nie tylko kryzysowi bankowemu, ale i kryzysowi zadłużenia jednocześnie.

30. Polski sektor bankowy **ma solidną pozycję kapitałową i płynnościową, niemniej cechuje go wyraźna podatność na ryzyko geopolityczne**. Wynika to z kombinacji następujących czynników: bliskości geograficznej do konfliktów (szczególnie Ukrainy) oraz wrogich krajów (Rosji i w pewnym stopniu także Białorusi), a także wysokiej ekspozycji na obligacje skarbowe oraz nieoptymalnego *policy mix*. W warunkach wojny hybrydowej (poniżej progu artykułu 5 NATO) można spodziewać się prób testowania odporności Polski na realizację poszczególnych rodzajów ryzyka geopolitycznego.

31. Można spodziewać się takich incydentów jak np. cyberataki na polski system bankowy, działania dezinformacyjne, czy nawet ataki na infrastrukturę krytyczną. Rodzi to konieczność wypracowania skutecznych metod i sposobów ograniczania ryzyka geopolitycznego, a także stawia przed polskimi bankami określone wyzwania. Spośród nich warto zwrócić uwagę na następujące obszary: (1) aspekty techniczne; (2) kwestie finansowania obronności; (3) kwestie finansowania energetyki oraz (4) warunki wojny hybrydowej.

32. Formułując rekomendacje odnośnie do przygotowania polskiego sektora bankowego na scenariusze, w jakich materializuje się ryzyko geopolityczne w odniesieniu do samych instytucji bankowych zasadne wydają się następujące działania:

- **Dywersyfikacja i redundancja infrastruktury krytycznej** – banki powinny geograficznie rozproszyć centra danych i systemy backupowe poza region potencjalnych konfliktów. Kluczowe jest posiadanie redundantnych systemów w lokalizacjach zachodnich (np. Frankfurt, Londyn) oraz zabezpieczenie łączności poprzez alternatywne kanały komunikacji; warto także wykorzystać rozwiązania chmurowe.
- **Działania na rzecz bezpiecznego i niezakłóconego dostępu do gotówki** – wypracowanie planów zarządzania zwiększonym popytem na gotówkę w kryzysie; zabezpieczanie fizycznych łańcuchów dostaw i przechowywania znaków pieniężnych; współpraca NBP z bankami, firmami transportującymi i zabezpieczającymi gotówkę; wyważenie przez banki efektywności redukcji infrastruktury gotówkowej z względami stabilności systemu; działalność edukacyjna podnosząca świadomość znaczenia gotówki w sytuacjach kryzysowych.
- **Zróżnicowane bufory płynnościowe i rezerwy** – utrzymywanie rezerw nie tylko w PLN i EUR/USD, ale także w walutach i aktywach, które można traktować jako safe havens (CHF, JPY, ale i złoto, zwłaszcza w kontekście możliwości, jakie daje w tym zakresie Basel III oraz potencjalny Bretton Woods III).
- **Konsekwentna implementacja zapisów DORA, MiCA i NIS2** – regulacje te powinny być postrzegane jako fundament odporności; należy jednak unikać tzw. *gold-plating*, mogącego stanowić tzw. *overkill* dla odporności systemowej na ryzyko geopolityczne.
- **Dbałość o suwerenność i bezpieczeństwo technologiczne** – eliminacja wszelkich zależności od dostawców z krajów potencjalnie wrogich lub niestabilnych; preferowanie rozwiązań europejskich lub z krajów sojuszniczych, zwłaszcza w infrastrukturze krytycznej.
- **Sektorowa analiza wrażliwości** – identyfikacja (na bazie ciągłej) branż szczególnie narażonych na konkretne ryzyka geopolityczne (energetyka, transport, przemysł zależny od importu surowców z Rosji/Chin). Różnicowanie wymogów kapitałowych i limitów koncentracji.

- **Transparentna komunikacja z klientami** – przygotowanie komunikatów kryzysowych wyjaśniających potencjalne ograniczenia w dostępie do usług, zamrożenia transakcji w przypadku sankcji, procedury ochrony depozytów; dbałość o przejrzystość decyzji i reputację. Wdrożenie sektorowego protokołu reagowania na atak informacyjny.
- **Utworzenie w bankach** (przynajmniej w tych szczególnie narażonych na ryzyko geopolityczne) **stanowiska Chief Geopolitical Risk Officer**. Osoba taka byłaby odpowiedzialna za integrację informacji geopolitycznych i działań w tym zakresie ze strategicznymi decyzjami i działaniami banku w określonych obszarach.

33. W odniesieniu do ogólnych ram funkcjonowania sektora bankowego można sformułować następujące rekomendacje dla regulatorów (Parlament, KNF) i decydentów (w szczególności ministerstw: finansów i gospodarki, obrony narodowej, funduszy i polityki regionalnej) w zakresie ograniczania konsekwencji zrealizowania się ryzyka geopolitycznego:

- Stworzenie kompleksowego modelu długotrwałej współpracy między 4 grupami podmiotów (rząd, przedsiębiorstwa prywatne i państwowe z sektora obronnego, banki komercyjne (państwowe i prywatne), ZBP, KNF). Celem tych działań ma być wsparcie bezpieczeństwa narodowego i rozwój polskiego sektora obronnego, gdyż niezbędne jest wykorzystanie – poprzez krajowy system bankowy – kapitału prywatnego do modernizacji tego sektora.
- Regularne spotkania merytoryczne dot. współpracy między tymi podmiotami organizowane przez właściwe ministerstwa.
- Wprowadzenie programu dot. zabezpieczenia finansowania długoterminowych inwestycji poprzez KUKE albo BGK, w celu ograniczenia ekspozycji banku na klienta lub na dany projekt (projekty w sektorze zbrojeniowym są długoterminowe i wymagają wielkiego finansowego zaangażowania).
- Wprowadzenie gwarancji (KUKE, BGK, rząd) na zawarte kontrakty zbrojeniowe z zagranicą, co chroni producentów przed ryzykiem braku płatności od zagranicznych klientów.
- Ustalenie zasad raportowania banków do KNF w przypadku finansowania projektów inwestycyjnych przedsiębiorstw z sektora zbrojeniowego objętych klauzulą informacji niejawnych.
- Zapewnienie długoterminowości kontraktów na zakup sprzętu od polskich przedsiębiorstw przez Skarb Państwa, tak aby zabezpieczyć zyskowność inwestycji i terminową spłatę kredytów.
- Stworzenie systemowego wsparcia (specjalne programy oferowane przez BGK, PFR) dotyczącego finansowania, zabezpieczenia kredytów banków udzielanych startupom z sektora MŚP, które inwestują w projektowanie i produkcję innowacyjnych produktów *dual-use*.
- **Obniżenie istniejących ciężarów fiskalnych**, w tym rozważenie (trwałej lub czasowej) obniżki podatku CIT dla banków w okresach wysokiej ekspozycji na ryzyko geopolityczne, a także w okresach wzmożonego uczestnictwa w finansowaniu wydatków związanych z obronnością
- **Dodatkowe gwarancje dla instytucji bankowych** zaangażowanych aktywnie w finansowanie zbrojeń oraz inwestycji energetycznych
- Zaoferowanie przez banki rachunków oszczędnościowo-inwestycyjnych dla konsumentów, wsparte ulgami podatkowymi przez państwo, aby zachęcić do inwestowania i rozwijać krajowy rynek kapitałowy.
- Rozważenie przez rząd i KNF zmniejszenia ograniczeń w rozwoju zdolności banków do akumulacji kapitału (co ogranicza ich możliwości udzielania kredytów) związanych z regulacjami i obecną konstrukcją podatku bankowego.
- Rozważenie zmian w regulacjach dotyczących limitów zaangażowania banku/konsorcjum banków w dany projekt z sektora obronnego, z ekspozycją na Skarb Państwa (nowe rozwiązania np. w ustawie o obronie Ojczyzny, dodatkowe gwarancje ze strony państwa w przypadku przekroczenia limitów).

34. Ryzyko geopolityczne w przeważającej mierze ma charakter egzogeniczny względem systemu bankowego. Jest też trudne do prognozowania i nie poddaje się hedgingowi. Z tych względów, **możliwości samych banków zabezpieczania się przed tym ryzykiem są z natury rzeczy ograniczone**. W pierwszej kolejności kluczowe są tu zatem działania na szczeblu całego państwa (decyzje polityczne, udział w międzynarodowych organizacjach i instytucjach, polityka

makroekonomiczna, polityki sektorowe), a także koordynacja działań poszczególnych organów, instytucji i decydentów.

35. Z uwagi na trwające gwałtowne zmiany technologiczne, jednym z węzłowych obszarów w kontekście ryzyka geopolitycznego są obecnie kwestie dotyczące cyberbezpieczeństwa, cyberataków, odpowiedniego uregulowania cyfrowych aktywów (w tym zwłaszcza kryptowalut), zapewnienia redundancji systemów. Warto wskazać, że polski system bankowy można uznać za jeden z najbardziej innowacyjnych pod względem technologicznym, co najmniej w regionie.

36. Zapewnienie trwałej i większej odporności na ryzyko geopolityczne wymaga zrozumienia i odpowiedniego wyważenia (systemowych, długofalowych) korzyści płynących z jego zapewnienia z koniecznością ponoszenia (indywidualnych, krótkookresowych) kosztów w tym zakresie przez poszczególne instytucje bankowe.

37. Jako **scenariusze stress testów** w raporcie (aneks) przedstawiono, wraz z uzasadnieniem ich rozważenia, potencjalnym przebiegiem wydarzeń, głównymi kanałami wpływu na banki oraz następstwami (ogólnymi i sektorowymi) następujące sytuacje w zakresie realizacji ryzyka geopolitycznego:

- Eskalacja wojny na Ukrainie
- Wycofanie się USA z Europy
- Kryzys i fragmentacja Unii Europejskiej
- Cyfrowe euro – fiasko implementacji
- Waluta BRICS – The Unit (dekompozycja systemu walutowego)
- Cyberatak na krajową infrastrukturę płatniczą
- Cyberatak na infrastrukturę IT USA
- Kryzys zaufania do AI w sektorze finansowym
- Kryzys energetyczny 2.0 – permanentna drożyzna energii
- Dezintegracja łańcuchów dostaw – nowy protekcjonizm
- Eskalacja konfliktu wokół Tajwanu z szokiem podażowym
- *Perfect Storm* (kumulacja negatywnych zdarzeń/wyzwalaczy ryzyka geopolitycznego)

Wstęp

Ostatnie lata na ogół postrzega się jako okres wzmożonej niestabilności i niepewności. W funkcjonowaniu rynków i całych gospodarek, życiu społecznym i politycznym, a nawet w kulturze i sferze mentalnej obywateli poszczególnych państw, regionów czy gospodarki światowej traktowanej jako całość, występuje szereg niekorzystnych trendów i procesów. Powszechne i częste jest także pojawianie się kolejnych nieprzewidzianych (ang. *unprecedented*) wydarzeń, odpowiadających talebowskiej koncepcji „czarnego łabędzia" (Taleb, 2020), czy zaliczanych do tzw. „szarych nosorożców" (ang. *grey rhinos*) (Wucker, 2016).

Począwszy od (globalnego) kryzysu finansowego z lat 2007–2009 i jego, zdaniem wielu autorów, do dziś trwających skutków i nierozwiązanych problemów strukturalnych poprzez następujące po nim Wielką Recesję (ang. *Great Recession*), kryzys zadłużenia w strefie euro, tendencje deflacyjne, pandemię COVID-19, aż po rosyjską agresję na Ukrainę, widoczne jest stopniowe (a czasem skokowe) wygaszanie epoki „końca historii" i dekonstrukcji światowego ładu. Uwzględniwszy także takie kwestie jak: zmieniający się układ sił w gospodarce światowej, rosnące nierówności, kwestie klimatyczne, tendencje deglobalizacje i problemy z funkcjonowaniem łańcuchów dostaw, zaburzenia w funkcjonowaniu systemów monetarnych, gwałtowne przemiany strukturalne będące następstwem zmian technologicznych i społecznych, uzasadnione jest, jak się wydaje, nazywanie tych niespełna dwóch ostatnich dekad epoką polikryzysów (ang. *policrises*) czy permakryzysu (ang. *permacrisis*)[1].

Oczywiście, nie brakowało w historii okresów, gdzie natężenie niekorzystnych zjawisk i procesów było równie, a może nawet bardziej znaczące. Niemniej, jak się wydaje, skalę, zakres oraz tempo przemian gospodarczych i społecznych zachodzących w ostatnich latach, a także kompleksowość i wagę konsekwencji obserwowanych zjawisk i procesów, można uznać za bezprecedensowe – tym bardziej, iż z uwagi na postęp środków telekomunikacji i szybszy przepływ informacji, wszystkie te zjawiska i procesy są transparentne, zachodząc na oczach społeczeństw i będąc szeroko oraz niejako „na żywo" komentowane. Ponadto, kontrast jest tu tym większy, że ten okres niestabilności i niepewności nastąpił niedługo po ogłoszeniu „końca historii", w warunkach tzw. świata jednobiegunowego, cechującego się dominacją jednego światowego supermocarstwa (USA), szczytem tendencji globalizacyjnych, unifikacji i integracji gospodarczej oraz politycznej. Warto tu przypomnieć, że jeszcze na początku XXI wieku mówiono o „śmierci cyklu koniunkturalnego", „śmierci inflacji" i uzyskaniu przez ekonomistów recept na ogólny dobrobyt i pomyślność, co znalazło wyraz w okresie tzw. Wielkiej Moderacji (*Great Moderation* – zob. Bernanke, 2004).

Jednym z elementów tej rosnącej złożoności, a jednocześnie kruchości warunków funkcjonowania całych gospodarek, poszczególnych rynków i branż, jak i pojedynczych instytucji czy podmiotów jest obserwowany prymat (geo) polityki nad gospodarką (Mishra i Sen, 2024). Z tym zaś ściśle wiąże się dramatyczny wręcz wzrost tzw. ryzyka geopolitycznego. Zjawisko to, najogólniej rozumiane jako ryzyko związane z napięciami wpływającymi na normalny i pokojowy przebieg stosunków międzynarodowych (np. ataki terrorystyczne, cyberataki, konflikty kinetyczne i gospodarcze, problemy z łańcuchami dostaw, kryzysy energetyczne i migracyjne)[2], jest czynnikiem coraz silniej wpływającym, niezależnie od innych podmiotów i sfer gospodarki, także na instytucje i rynki finansowe poszczególnych krajów. W zglobalizowanym świecie, w którym współzależności międzynarodowe urosły do nieznanych wcześniej rozmiarów, ryzyko geopolityczne staje się kluczowym czynnikiem, które należy brać pod uwagę. Znaczenie granic, odległości oraz relacji krajów o takim samym systemie gospodarczym i politycznym zwiększa się. Poszczególne podmioty gospodarujące (a także całe państwa) muszą się dostosowywać i szukać nowych przewag.

Dotyczy to także – a może nawet przede wszystkim – podmiotów ze sfery finansowej, będących wcześniej w ścisłej awangardzie procesów internacjonalizacyjnych oraz technologicznych. Instytucje te, zwłaszcza największe spośród nich, dalece wykraczają poza swoje rynki macierzyste, zarówno pod względem struktury geograficznej, oferty, jak i kanałów dystrybucji. To zaś czyniło banki, ubezpieczycieli czy fundusze inwestycyjne podatnymi na zmiany warunków międzynarodowych. Stąd, można zaryzykować stwierdzenie, że ryzyko geopolityczne staje się

1 Koncepcje te, jako kluczowe z punktu widzenia problematyki raportu, zostaną szerzej przedstawione w części 1.

2 Pojęcie to zostanie szczegółowo przedstawione w części 1.

jednym z głównych parametrów, jakie podmioty te muszą uwzględniać planując swoje operacje. Tego typu optykę przyjmuje w swoich opracowaniach większość znaczących organizacji i instytucji międzynarodowych, zarówno komercyjnych, jak i publicznych (zob. np. European Parliament, 2025; EBC, 2025, EBA, 2024; IMF, 2025, Ernst&Young, 2025).

Tymczasem, mimo swojego znaczenia, źródła, mechanizmy i kanały oddziaływania ryzyka geopolitycznego oraz konsekwencje, jakie ma ono – i może mieć – dla sektora bankowego nadal nie są dokładnie rozpoznane. Utrudnia to zaprojektowanie właściwych rozwiązań, mających ograniczyć to ryzyko oraz zapobiec negatywnym skutkom, jakie jego realizacja miałaby dla instytucji bankowych. Kwestia jest o tyle skomplikowana, że ryzyko geopolityczne z samej swojej natury jest czynnikiem egzogenicznym dla banków (być może z pewnymi wyjątkami w odniesieniu do największych instytucji globalnych); mogą one w odniesieniu do tego ryzyka przybierać raczej postawy głównie reaktywne.

Z tych względów zasadne jest przenalizowanie zagadnienia ryzyka geopolitycznego i jego (potencjalnego) wpływu na funkcjonowanie i stabilność systemu bankowego. Należy także rozważyć możliwe sposoby ograniczania wpływu tego ryzyka i/lub kosztów takich działań. Odnoszą się one do wielu aspektów funkcjonowania banków, w tym zwłaszcza do zapewnienia skutecznych regulacji i ram instytucjonalnych, bezpieczeństwa cybernetycznego, ciągłości procesów, ochrony środków klientów, niezakłóconego dokonywania płatności bezgotówkowych, odpowiedniego zaopatrywania w pieniądz gotówkowy, itp. W rozważaniach autorzy, oprócz zapewnienia podstaw teoretycznych i prawnych kwestii ryzyka geopolitycznego i jego wpływu na sektor bankowy, będą sięgali do przykładów z praktyki.

Celem raportu jest zatem charakterystyka zjawiska ryzyka geopolitycznego i rozważenie w tym kontekście poziomu bezpieczeństwa sektora bankowego w Polsce. Szczególną uwagę zwrócono na źródła ryzyka geopolitycznego (ze szczególnym uwzględnieniem tzw. cyberzagrożeń), jego rodzaje, mechanizmy (kanały) wpływu na instytucje bankowe, konsekwencje oraz sposoby zarządzania tym ryzykiem. Sformułowane zostaną także rekomendacje dla polskich instytucji bankowych i decydentów odnośnie do strategii i działań względem ryzyka geopolitycznego.

Całość składa się z czterech części. W pierwszej opisano teoretyczne kwestie dotyczące geopolityki i ryzyka geopolitycznego. Warto tu podkreślić, iż z uwagi na obszerność i złożoność rozpatrywanych w raporcie problemów, koncepcji i idei, ich prezentacja z natury rzeczy jest dość syntetyczna, gdyż każda z nich z osobna mogłaby stanowić przedmiot osobnego raportu. W części drugiej opisano wybrane manifestacje ryzyka geopolitycznego w sferze monetarnej i finansowej: cyberzagrożenia dla sektora finansowego, konsekwencje tego ryzyka dla rynku kryptowalut, przepływy kapitałowe i bezpośrednie inwestycje zagraniczne oraz kwestie funkcjonowania sfery gotówkowej i ryzyka odpływu depozytów. Część trzecia dotyczy już stricte ryzyka geopolitycznego w działalności banków – mechanizmów, konsekwencji i sposobów ograniczania w systemach bankowych. Przedmiotem rozważań w części czwartej jest natomiast polski system bankowy w kontekście ryzyka geopolitycznego. Przybliżono występowanie i nasilenie tego ryzyka w Polsce, swoiste cechy polskiego systemu bankowego w kontekście ryzyka geopolitycznego, a także wybrane wyzwania stojące przed krajowym systemem bankowym w kontekście ryzyka geopolitycznego. W końcowej części przedstawiono rekomendacje w zakresie ograniczania tego ryzyka i skutków jego wystąpienia.

Część 1. Geopolityka i ryzyko geopolityczne – ramy koncepcyjne

1.1. Geopolityka – pojęcie, istota, zakres

Geopolityka to, najogólniej, rozumienie zjawisk ekonomicznych i politycznych z perspektywy geograficznej. Można rozumieć ją jako obszar badań na przecięciu się geografii, polityki, strategii, ekonomii i historii, w ramach którego autorzy zajmują się tym, jak czynniki geograficzne (takie jak granice, zasoby naturalne, demografia przestrzenna, położenie strategiczne, itp.) kształtują i wpływają na globalne sprawy polityczne (Palgrave, 2024). Inaczej mówiąc, jest to podejście do międzynarodowej polityki, które kładzie szczególny nacisk na rolę terytorium (lokalizacja, dostęp do oceanu/mórz, przebieg granic, kraje sąsiadujące) i zasobów naturalnych w kształtowaniu sytuacji politycznej i gospodarczej państwa. Można zatem powiedzieć, że jest to „wspólny projekt" geografii politycznej i stosunków międzynarodowych (Criekemans, 2023).

Pojęcie geopolityki pojawiło się z końcem XIX wieku[3], kiedy obserwowano narastające współzawodniczenie pomiędzy najpotężniejszymi państwami świata o wpływy polityczne, dostęp do zasobów gospodarczych oraz kolonie. Wraz z ewolucją gospodarki, społeczeństw i ustrojów, zmieniały się zarówno podmiot, jak i przedmiot geopolityki. Współcześnie, co istotne także z punktu widzenia niniejszego opracowania, geopolityczne myślenie nie jest tylko przynależne państwom[4], ale też innym podmiotom (aktorom, agentom) nie-państwom (instytucjom finansowym i niefinansowym, potentatom technologicznym – tzw. BigTech, organizacjom międzynarodowym, stowarzyszeniom, w tym stowarzyszeniom handlowym i militarnym). W rezultacie tych przemian kwestie geopolityczne skomplikowały się, a osiąganie poszczególnych celów wymaga uwzględniania większej liczby zmiennych i zależności niż zakładali tacy „ojcowie" geopolityki jak Rudolf Kjellen, Halford Mackinder czy uznawany za twórcę polskiej szkoły geopolityki Eugeniusz Romer.

W ostatnich dekadach, jak to zostanie opisane w następnej sekcji, kwestie geopolityczne wskutek splotu czynników ekonomicznych, politycznych i społecznych dodatkowo zyskały na znaczeniu, głębi i złożoności[5]. Można tu wskazać w szczególności trzy daty: rok 1989, a więc koniec zimnej wojny i początek dominacji USA jako jedynego mocarstwa globalnego, rok 2007 czyli wybuch kryzysu finansowego, nazywanego powszechnie globalnym kryzysem finansowym – wydarzenie, które można postrzegać jako kres hegemonii umownie nazywanego Zachodu, i wreszcie rok 2019, czyli wybuch w chińskim mieście Wuhan epidemii koronawirusa SARS-2, która w marcu następnego roku została uznana za pandemię. Wszystkie te wydarzenia niosły za sobą bardzo znaczące następstwa, akcentując jednocześnie wagę poszczególnych elementów i mechanizmów stanowiących obszary badawcze geopolityki.

Najogólniej, geopolityka analizuje wymiary i czynniki, determinujące, w jaki sposób państwa funkcjonują i współdziałają na arenie międzynarodowej. Wyróżnić można sześć takich wymiarów i określających je czynników (Cope, 2024). Syntetycznie ujęto je na Rysunku 1.

Wymiar **geografii** obejmuje takie czynniki jak granice, dostęp do zasobów naturalnych, bliskość/odległość do/od innych państw, strategiczną lokalizację na szlakach wodnych, czy wreszcie tzw. *choke points*, czyli kluczowe, krytyczne węzły w globalnym systemie, w których pojedynczy kraj lub podmiot może sprawować kontrolę, tworząc swoistą dźwignię ekonomiczną lub militarną, za pomocą której może egzekwować określone zachowania innych graczy (lub zapobiegać im)[6]. Ze wszystkich wymiarów geopolityki ten można uznać za najbardziej „klasyczny" i elementarny. Co istotne, mimo rozwoju nowoczesnych technologii i gospodarki cyfrowej, tra-

3 Jako pierwszy użył go Rudolf Kjellen w 1899 r. w pracy „Studier öfver Sveriges politiska gränser".

4 Tradycyjnie, państwo utożsamia się z jego władzami politycznymi i gospodarczymi. W raporcie pisząc o „państwie" autorzy mają na myśli rząd (ang. *government*), mając na względzie, że w praktyce poszczególnych państw możliwe są rozmaite rozwiązania ustrojowe i instytucjonalne. Przykładowo, typowa dla współczesnych gospodarek rynkowej jest niezależność banku centralnego, z którą, obok licznych zalet, wiążą się również wątpliwości, w tym bardzo istotne z punktu widzenia demokracji i polityki zagadnienie odpowiedzialności demokratycznej (ang. *accountability*) niezależnych banków centralnych. Mianowicie, w skrajnej sytuacji instytucje te mogą prowadzić politykę nakierowaną na realizację celów innych, niż cele rządu i/lub społeczeństwa (zob. np. Fraser, 2015; Wojtyna, 2002).

5 Warto odnotować nasilenie, czy wręcz swoiste odrodzenie dyskusji geopolitycznych także w polskiej debacie publicznej.

6 Przykładami są tu m. in. Cieśnina Ormuz czy Cieśnina Malakka.

dycyjne czynniki lokalizacyjne bynajmniej nie tracą na znaczeniu. Nadal istotnie wpływają one na politykę zagraniczną danego kraju i jego pozycję na arenie międzynarodowej.

Rysunek 1. Wymiary geopolityki

Źródło: Opracowanie własne na podstawie: Cope (2024).

Na wymiar **dynamiki siły** (ang. *power dynamics*) składają się czynniki określające podział siły między krajami, takie jak: potencjał militarny, potęga gospodarcza (w tym poziom dochodu narodowego, jakość i odporność instytucji, stabilność i rozmiary systemu finansowego), technologia i tzw. „soft power". Elementy te mają wpływ na równowagę sił na arenie międzynarodowej, globalną politykę i decyzyjność państwa. W bezpośredni sposób określają one konkurencyjność danego państwa czy bloku państw.

W wymiarze **rywalizacji (konkurowania) o strategiczne zasoby** rozpatruje się dostępność zasobów takich jak: woda, ropa, minerały (w tym metale ziem rzadkich, kluczowe w ostatnich latach z uwagi na ich rolę w produkcji urządzeń wysokiej technologii), ziemia, itp. Możliwość dysponowania zasobami, bądź ich rzadkość lub w ogóle brak w danym państwie określa potencjalny konflikt bądź współpracę pomiędzy krajami, a tym samym kształtuje politykę międzynarodową. Tego typu kwestie zyskały na znaczeniu w obliczu pandemii i związanych z nią zakłóceń funkcjonowania łańcuchów dostaw oraz wskutek nasilenia tendencji deglobalizacyjnych, o czym będzie szerzej mowa w punkcie 1.2.

Wymiar **strategicznych interesów** jest określany przez formułowane w danym państwie założenia dotyczące bezpieczeństwa narodowego, wpływów kraju w regionie, uwarunkowań, płaszczyzn i instrumentów przeciwstawienia się krajom-konkurentom, a także stawianych celów gospodarczych, czy szerzej – rozwojowych. Sformułowanie strategicznych interesów jest punktem wyjścia wszelkich dyplomatycznych, militarnych i handlowych inicjatyw oraz działań. Ponadto, stanowi warunek *sine qua non* ich skuteczności.

Wymiar **aliansów i koalicji** obejmuje wszelkie działania (oraz ich uwarunkowania) mające na celu zbudowanie wspólnego bloku/bloków krajów z intencją poparcia i realizacji wspólnych celów przez dany sojusz lub przeciwdziałania wspólnym zagrożeniom. Formy takich aliansów czy koalicji mogą być rozmaite, od dość ogólnych umów o współpracy politycznej i/lub gospodarczej, po mocno sformalizowane struktury, takie jak NATO, czy UE.

Ostatnim, szóstym wymiarem jest **globalne zarządzanie**. Obejmuje on takie czynniki oraz instytucje jak ONZ, WTO, a także różnego rodzaju regionalne ugrupowania, bilateralne i multilateralne porozumienia, które regulują stosunki między państwami,

ograniczają konflikty, promują współpracę i próbują rozwiązać problemy pojawiające się we wzajemnych relacjach. W kontekście tematyki raportu warto zaznaczyć, że czynnikiem składającym się na wymiar globalnego zarządzania byłoby także funkcjonowanie międzynarodowego systemu walutowego. Można by tu również, jak się wydaje, ująć działalność międzynarodowych organizacji i instytucji finansowych, takich jak MFW czy BIS.

Można zauważyć, że poszczególne wymiary są ze sobą ściśle powiązane. Widać także wyraźnie, że poczesne miejsce w rozważaniach geopolitycznych zajmują kwestie gospodarcze, w tym także funkcjonowanie sfery monetarnej i systemów finansowych.

Z zestawienia tych sześciu wymiarów geopolityki wynika ponadto, że w architekturze geopolitycznej najważniejszymi graczami (podmiotami) są państwa. Do II wojny światowej dominowały one w tzw. architekturze geopolitycznej[7], będąc potęgami militarnymi, kolonialnymi, czy wręcz imperiami walczącymi o wpływy i zasoby. Po tej wojnie wykształcił się swoisty nowy porządek świata, w którym pojawiły się takie organizacje międzynarodowe, jak: Międzynarodowy Fundusz Walutowy (IMF) i Bank Światowy[8], ONZ, GATT i NATO. Niemniej, państwa (szczególnie te największe, najsilniejsze gospodarczo, ale też i te najbardziej innowacyjne) pozostały głównymi podmiotami w mozaice geopolitycznej, dysponując zasadniczo najszerszym wachlarzem instrumentów i działań oraz będąc jednostkami, w gestii których znajduje się najwięcej zasobów.

Niemniej, od lat 90. ubiegłego wieku, czyli w okresie wzmożenia globalizacji architektura geopolityczna zmieniała się dynamicznie. W rezultacie, współcześnie, wskutek procesów globalizacji, finansyzacji, postępu technologicznego, a także czynników natury ideologicznej i kulturowej jako ważnych graczy w geopolitycznej grze sił trzeba – na równi z państwami – rozpatrywać też inne podmioty oraz wzajemne ich zależności. W szczególności, należy tu wskazać regionalne organizacje, korporacje transnarodowe (finansowe i niefinansowe), globalne media, przedsiębiorstwa technologiczne, globalne serwisy społecznościowe czy organizacje międzynarodowe.

Znaczenie tych nowych graczy wzrosło ogromnie w ostatnich dwóch dekadach. W wielu przypadkach odgrywają one nawet większą rolę i dysponują większymi zasobami, niż wiele państw narodowych, potrafiąc wymusić na nich określone, korzystne dla siebie decyzje. W szczególny sposób dotyczy to wielkich globalnych firm technologicznych, określanych mianem podmiotów tzw. BigTech. Zazwyczaj używa się tu terminu GAFAM, który odnosi się do 5 firm technologicznych ze Stanów Zjednoczonych: Google (Alphabet), Amazon, Facebook (Meta), Apple i Microsoft. Jednak jako Big Tech należy również traktować duże chińskie firmy IT, takie jak Baidu, Alibaba, Tencent ByteDance i Xiaomi, mniejsze firmy technologiczne o wysokich wycenach, takie jak Netflix i Nvidia, nowych potentatów z zakresu AI, takich jak OpenAI i Anthropic, a także przedsiębiorstwa nie stricte technologiczne, ale z branży high-tech, takie jak Space X czy Tesla. Podmioty te ogromnie się rozwinęły w wyniku tzw. Czwartej Rewolucji Przemysłowej (Schwab, 2016), stając się zwiastunami nowej ery informacyjnej i jednymi z najważniejszych graczy w światowej gospodarce. Po pandemii COVID-19 firmy Big Tech jeszcze bardziej wyprzedziły firmy z „tradycyjnych" branż. Podmioty te prowadzą wiele bardzo zróżnicowanych działalności biznesowych, których podstawą są szeroko rozumiane nowe technologie. W literaturze formułuje się wręcz poglądy mówiące o nowym etapie funkcjonowania kapitalizmu, czy wręcz nowym modelu ustrojowym, nazywanym „technofeudalizmem"[9] (Kotkin, 2020; Morozow, 2014; Warufakis, 2024; Zuboff, 2018). Z punktu widzenia problematyki raportu należy z kolei podkreślić, że z tymi podmiotami wiążą się nowe rodzaje ryzyka.

Charakterystyczne jest, że, że widocznym trendem w działaniach firm zaliczanych do Big Tech jest ich ekspansja na rynki finansowe. Podmioty te starają się bezpośrednio świadczyć usługi finansowe lub oferować swoim klientom produkty bardzo zbliżone do produktów finansowych. Dzięki przewadze technologicznej i informacyjnej mogą przy tym świadczyć usługi na dużo bardziej korzystnych warunkach.

Mając na względzie pojawienie się wszelkich nowych graczy, trzeba jednocześnie pamiętać, że podstawą stosunków międzynarodowych i geopolityki pozostaje dalej **państwo**, definiowane przez granice, które

7 „Geopolityczna architektura" jest terminem używanym do określenia sposobów, w jaki państwa i inni gracze „niepaństwowi" (przedsiębiorstwa, banki, instytucje finansowe, organizacje międzynarodowe) uzyskują dostęp do zasobów, a także zarządzają i regulują „przecięcia" terytoriów i przepływów (towarów i usług, kapitału, ludzi, technologii, idei), a tym samym ustanawiają granice między wnętrzem/zewnętrzem, obywatelem/obcym i krajowym/międzynarodowym (Dodds, 2007).

8 Obie te instytucje powstały w następstwie konferencji w Bretton Woods w 1944 r. Celem obu instytucji miało być wspieranie międzynarodowej stabilności gospodarczej i dostarczanie funduszy na odbudowę powojennych gospodarek narodowych.

9 Jak jednak pokazały doświadczenia ostatnich lat, tego typu transnarodowe korporacje jednak pozostają związane z krajem macierzystym, realizując, niezależnie od swoich celów, jego agendę geopolityczną.

są manifestacją suwerenności i stanowią barierę (bądź nie) dostępu do niego. Według definicji ONZ, respektującej wcześniejszą konwencję z Montevideo z 1933 r., państwo jest podmiotem, który spełnia określone kryteria: posiada stałą populację, określone terytorium, rząd i możliwości nawiązywania stosunków z innymi państwami[10]. W tradycyjnej geopolityce to państwo było w centrum i jest tak do dzisiaj, nawet mimo wspominanych nowych podmiotów geopolitycznej architektury oraz faktu, iż współczesny świat charakteryzuje się coraz większą współzależnością przepływów kapitału, handlu, osób, idei, oraz technologii. Oczywiście, znaczenie poszczególnych państw różni się, a przy tym ewoluuje. Zmieniają się również globalny układ sił, znaczenie poszczególnych regionów oraz strefy wpływów. Jeśli chodzi o państwa, to w centrum uwagi dalej pozostają USA i aspirujące do roli hegemona Chiny. Są to największe pod względem gospodarczym, militarnym, populacyjnym państwa uczestniczące w wyścigu gospodarczym i technologicznym (ostatnio w szczególności w zakresie AI) (zob. np. Alison, 2018; Sanger i Brooks, 2005).

Oprócz państwa, centralną kwestią dla zrozumienia geopolityki jest **władza**, w kontekście geopolityki rozumiana jako możliwość wpływu z pozycji siły na inne podmioty, egzekwowania pewnych decyzji, zmuszania do pewnych działań. Źródłem tej siły może być: potęga militarna, monopol na technologię, dostęp do surowców strategicznych, kontrola nad szlakami handlowymi, posiadanie waluty rezerwowej, itp. Władza może być w posiadaniu: rządzących państwami (demokratycznymi lub dyktatorskimi), korporacji transnarodowych finansowych i niefinansowych, właścicieli ważnych technologii (wspomniane korporacje Big Tech), właścicieli strategicznych surowców naturalnych, organizacji międzynarodowych (m.in. WTO, WB, IMF). Identyfikacja wielości podmiotów posiadających władzę oraz źródeł tej władzy pokazuje, jak ograniczona została współcześnie rola pojedynczego państwa. Często przedsiębiorstwa dysponujące zasobami rzadkimi, technologią czy kapitałem niejako „wymykają się" krajowym jurysdykcjom i regulatorom. Dotyczy to również instytucji finansowych, zwłaszcza globalnych banków, ubezpieczycieli, czy funduszów inwestycyjnych. Już w tym momencie można wskazać, że dla takich instytucji percepcja ryzyka geopolitycznego będzie odmienna, niż dla instytucji operujących wyłącznie na rynku macierzystym.

Z przedstawionych wymiarów geopolityki, determinujących je czynników oraz uwypuklenia kluczowej roli państw, rosnącej konkurencji prywatnych aktorów i zróżnicowanych mechanizmów władzy można zidentyfikować główne wyzwania, przed jakimi stoją współcześnie poszczególne państwa i bloki sojusznicze. Są to swoiste obszary problemowe, rozważane szeroko w opracowaniach i debatach geopolitycznych (zarówno międzynarodowych, jak i krajowych). Nie są to przy tym bynajmniej tylko zagadnienia teoretyczne, ale konkretne problemy, których rozwiązanie determinuje stabilność i porządek w gospodarce światowej, determinując przy tym podział siły, pracy i korzyści we wzajemnych stosunkach międzynarodowych. I tak, wśród najważniejszych punktów bieżącej agendy geopolitycznej można wskazać następujące elementy:

1. **Geografia i zasoby** – przebieg i bezpieczeństwo szlaków handlowych, dostęp do mórz, rozmieszczenie surowców naturalnych (ropa, gaz, minerały, metale ziem rzadkich), dostępność wody i żywności, kwestie klimatyczne.

2. **Strefy wpływów i rywalizacja państw** – konkurencja między wielkimi mocarstwami/blokami (USA, Chiny, Indie, Rosja, UE) o dominację w kluczowych regionach (Pacyfik, Europa Wschodnia, Bliski Wschód, Afryka).

3. **Szlaki handlowe i komunikacyjne** – kontrola nad cieśninami morskimi, kanałami, rurociągami i szlakami transportowymi (m.in. takie inicjatywy jak Nowy Jedwabny Szlak, Północna Droga Morska); potencjalna ekonomiczna eksploracja (bliskiego) kosmosu.

4. **„Rywalizacja" ustrojowa** – relacje między kapitalizmem finansowym a kapitalizmem przemysłowym; demokracja (liberalna) vs autorytaryzm.

5. **Bezpieczeństwo energetyczne** – zależności energetyczne, dywersyfikacja dostaw, transformacja energetyczna i jej wpływ na równowagę sił.

6. **Technologia i cyberprzestrzeń** – kontrola nad infrastrukturą cyfrową, standardami technologicznymi (5G, AI), bezpieczeństwo cybernetyczne jako nowa arena rywalizacji; fragmentacja internetu; FinTech i systemy płatności.

7. **Perspektywy przemian systemów pieniężnych i finansowych** – tendencje ku dedolaryzacji, kryptowaluty, neobankowość, poszukiwania nowej globalnej waluty rezerwowej.

10 Inna definicja państwa wg D.C. North to: granice geograficzne państwa stanowią obszar nakładania podatków (Por. North, 1981).

8. **„Wojny" walutowe i monetarne** – „weaponizacja" waluty, funkcjonowanie SWIFT i systemów konkurencyjnych; działania dewaluacyjne; sankcje finansowe; swoboda (lub brak) przepływów finansowych.

9. **Reorientacja handlu światowego** – „reshoring", „nearshoring" i „friendshoring" zamiast offshoringu; proliferacja barier handlowych (ceł oraz instrumentów pozataryfowych).

10. **Sojusze i instytucje międzynarodowe** – NATO, BRICS, SCO (Shanghai Cooperation Organization), UE; regionalne porozumienia: ich ewolucja i zmiana znaczenia w multipolarnym świecie; Północ vs Południe.

11. **Konflikty i punkty zapalne** – Tajwan, Ukraina, Bliski Wschód, Morze Południowochińskie jako obszary potencjalnych eskalacji.

Każdy z wymienionych obszarów wiąże się z konkretnymi tendencjami w zakresie kształtowania się zjawiska ryzyka geopolitycznego oraz konsekwencji, z jakimi wiąże się ono dla poszczególnych aktorów gry geopolitycznej, jak i dla podmiotów, dla których ryzyko to ma charakter egzogeniczny. Jak przy tym można zauważyć, obszary te stanowią złożoną, kompleksową mozaikę zagadnień czysto politycznych, technologicznych, jak i gospodarczych. Znajdują się wśród nich czynniki o charakterze *stricte* finansowym i pieniężnym, bezpośrednio wiążące się z funkcjonowaniem systemów bankowych (czy wręcz przez nie generowane), jak i takie, których oddziaływanie na te systemy ma mniej oczywisty (choć niemniej istotny) charakter.

Kończąc przedstawienie – z natury rzeczy bardzo syntetyczne – głównych aspektów dotyczących geopolityki, należy jeszcze uwypuklić kilka kwestii. **Po pierwsze**, należy wprowadzić rozróżnienie między geopolityką a geoekonomią[11]. Stanowią one dwie odrębne, choć ściśle powiązane perspektywy analizy międzynarodowych relacji rywalizacji, władzy i wpływów. Geopolityka, jak to przedstawiono, koncentruje się na geograficznych uwarunkowaniach polityki międzynarodowej i ich następstwach dla rywalizacji, konfliktów, sojuszy oraz pozycji międzynarodowej poszczególnych państw. Przedmiotem geoekonomii jest natomiast wykorzystanie przez kraje instrumentów ekonomicznych (walut, handlu, inwestycji, sankcji, kontroli nad łańcuchami dostaw, regulacji gospodarczych, itp.) do realizacji celów strategicznych (*Geoekonomia*, 2012). Geoekonomia jest zatem pewnym dopełnieniem geopolityki, opisującym wykorzystanie konkretnie instrumentów ekonomicznych dla realizacji polityki międzynarodowej. Można ją uznać wręcz za subdyscyplinę geopolityki (Lisiakiewicz, 2017). **Po drugie**, sama geopolityka, jak sygnalizowano, ewoluuje. W tradycyjnych analizach geopolitycznych (np. Mackindera czy Haushofera) zakłada się determinizm geograficzny – geografia determinuje politykę. Współczesne podejścia (m.in. geopolityka krytyczna czy geopolityka postmodernistyczna) akcentują raczej społeczne konstrukcje i narracje geopolityczne, zwracając uwagę na dynamikę przemian politycznych i społecznych (Jean, 2003; Potulski, 2012). **Po trzecie**, należy uwzględnić rozmaite poziomy analizy geopolitycznej: makro (globalne systemy i równowaga sił), mezo (regiony, bloki, sojusze) oraz mikro (lokalne konflikty o zasoby) oraz różny jej wymiar czasowy: struktury tzw. długiego trwania (geografia się nie zmienia), jak i dynamiczne procesy (technologia, globalizacja, zmiana klimatu) zmieniające znaczenie geografii. **Po czwarte**, bardzo wyraźne (co zresztą nie może dziwić) są powiązania geopolityki z polityką *per se*. Geopolitycy zajmują się doradztwem strategicznym, analizą ryzyka, często są zatrudniani przez rządy czy wojsko, tworzą finansowane z budżetu *think tanki*. Pojawia się zatem pytanie o relacje między nauką a strukturami władzy, o pewne swoiste „uwikłanie" geopolityki[12]. **Po piąte**, rozwój technologiczny bynajmniej nie unieważnił zagadnień geopolitycznych, a może nawet jeszcze je wzmocnił. Cyberprzestrzeń stała się jedną z ważniejszych domen, w jakich toczy się rywalizacja geopolityczna, a u podstaw wirtualnego świata nadal leżą „twarde" czynniki materialne.

11 Za twórcę terminu „geoekonomia" powszechnie w literaturze nauk społecznych uznaje się amerykańskiego stratega wojskowego, politologa i historyka Edwarda Luttwaka, który użył tego terminu po raz pierwszy w 1990 (Luttwak, 1990).

12 Osobną kwestią są obciążenia historyczne, związane z wykorzystywaniem geopolityki przez nazistów oraz bardzo prężnym funkcjonowaniem radzieckiej/rosyjskiej szkoły geopolitycznej, problemem eurocentryzmu w klasycznych analizach geopolitycznych, a także – bardziej współcześnie – potencjalnym legitymizowaniem i naukowym racjonalizowaniem przez geopolitykę polityki siły.

1.2. Przyczyny wzrostu znaczenia geopolityki po 1989 roku

Jak wspomniano w poprzedniej sekcji, znaczenie czynników geopolitycznych (jak i samej geopolityki jako nauki) w ostatnich latach znacząco wzrosło. Liczne współcześnie międzynarodowe konflikty polityczne, wojny w Europie, Afryce i Azji pokazują, że znaczenie geopolityki jest kluczowe. Nie brakuje opinii mówiących o znaczących zmianach strukturalnych w światowej gospodarce, wykształcaniu się nowego światowego układu sił, czy wręcz nadchodzącej trzeciej wojnie światowej (Khanna, 2022; Mahbubani, 2023 i 2025; Sanger i Brooks, 2025). 92052010674.

Renesans idei geopolitycznych był jednak widoczny już w ostatniej dekadzie XX wieku. Zarysowało się wówczas znaczne przyspieszenie procesów globalizacji, które zredefiniowały globalną architekturę geopolityczną. Właśnie **zjawisko globalizacji** było czynnikiem, który, paradoksalnie, wraz z przekraczaniem i zacieraniem granic między państwami oraz tworzeniem się globalnego rynku, podkreślił znaczenie poszczególnych wymiarów geopolityki. Mimo argumentów na rzecz globalizacji, przekonania, że wolny handel i współpraca gospodarcza sprzyjają wygaszaniu konfliktów zbrojnych, okazało się, że walka o wpływy polityczne, granice, niezależność pozostaje tak samo ważna jak zawsze. Co istotne, w dobie globalizacji konflikty, z uwagi na wszechogarniającą sieć wzajemnych powiązań[13] dotyczą wszystkich bez znaczenia czy bezpośrednio graniczą z danym krajem. Poprzez technologię, idee, transport, przepływy handlowe i kapitałowe oraz turystykę, miejsca i ludzie są ze sobą połączone i zależne. Oprócz pozytywnych następstw rodzi to także problemy[14].

W aspekcie ekonomicznym globalizację można traktować jako proces integrowania się gospodarek narodowych, dokonujący się poprzez rozszerzanie i intensyfikowanie wzajemnych powiązań produkcyjnych, handlowych i kapitałowych, czego następstwem staje się ogólnoświatowy system ekonomiczny o dużej współzależności. W systemie tym pogłębia się tendencja do traktowania – przez coraz większą liczbę podmiotów, w tym przedsiębiorstw – całego świata jako rynku zbytu.

Analizując genezę tego procesu, wyróżnić można trzy główne grupy czynników leżące u podstaw nowożytnej globalizacji, a w szczególności jej przyspieszenia na przełomie lat 80. i 90. ubiegłego wieku. Mianowicie, są to czynniki o **charakterze politycznym, ekonomicznym i technologicznym**. Rozpatrując te pierwsze, należy uwzględnić fakt, że dynamika globalizacji uległa wyraźnemu zwiększeniu wraz z upadkiem systemu socjalistycznego i gospodarki centralnie zarządzanej w Europie Środkowej i Wschodniej oraz w byłym ZSRR. Ważne znaczenie miało także rozpoczęcie reform gospodarczych w Chinach. Oznaczało to postępujące upodobnianie ustrojów gospodarczych (ale też politycznych) na świecie, wiązane z ówczesnym triumfem tzw. demokracji liberalnej[15].

W grupie czynników ekonomicznych, globalizację wiązano z nasilającą się podówczas liberalizacją gospodarczą zarówno wewnątrz krajów, jak i pomiędzy nimi. W tym procesie ważką rolę odegrały organizacje międzynarodowe (IMF, WB, WTO), które promowały rozwój gospodarki kapitalistycznej opartej na wolnym handlu i swobodnych przepływach kapitałowych[16]. Wzrosło również znaczenie regionalnych ugrupowań integracyjnych (NAFTA, ASEAN, UE). Ponadto swoje znaczenie wykazały rosnące w siłę korporacje transnarodowe (w tym globalne banki). Umożliwiły one integrację globalnej gospodarki poprzez swoje inwestycyjne i produkcyjne przedsięwzięcia. Efektem tego był obserwowany w latach 90. ubiegłego wieku historycznie największy wzrost obrotów handlowych oraz poziomu PKB w wielu krajach świata, a także wzrost udziału handlu zagranicznego (suma eksportu i importu) w PKB.

Trzecią grupą czynników, przyczyniających się do rozwoju globalizacji stały się zmiany wynikające z przyspieszenia postępu technologicznego, obserwowane od lat 60. XX w. i nasilające się z każdą kolejną dekadą. Zazwyczaj wiąże się je z tzw. trzecią, utożsamianą z komputerami i robotyką (lata 1970–2000),

13 Warto zasygnalizować tu bardzo ścisłe i wielopłaszczyznowe powiązania między krajowymi rynkami i systemami finansowymi, które po 2007 r. miały przyczynić się do tak masowego „rozlania się" (ang. *spillover*) na bardzo wiele rynków i państw kryzysu zapoczątkowanego na amerykańskim rynku kredytów *subprime*.

14 O współzależnościach jako źródle konfliktu pisał np. Mark Leonard (2002).

15 Właśnie w tym kontekście swoją, z perspektywy czasu mocno niefortunną, koncepcję „końca historii" sformułował Fukuyama (1992).

16 Swoistym ukoronowaniem tego podejścia było przyjęcie do WTO 11 grudnia 2001 r. Chin.

oraz czwartą rewolucją przemysłową, w której główne miejsce przypisuje się internetowi i szeroko pojętej cyfryzacji[17] (Groumpos, 2021; Ratajczak i Woźniak-Jęchorek, 2020). Z obu rewolucjami wiążą się takie zjawiska jak przełom teleinformatyczny, cyfryzacja i automatyzacja procesów produkcyjnych poprzez wprowadzenie elektroniki i technologii IT, rozwój internetu (społecznościowego, komercyjnego, semantycznego), analiza danych na niespotykaną wcześniej skalę (Big Data), internet rzeczy, robotyka, systemy cyberfizyczne umożliwiające autonomiczne i inteligentne zarządzanie produkcją. Czynniki te spowodowały gwałtowną zmianę w gromadzeniu, przetwarzaniu i przesyłaniu informacji oraz tworzeniu nowej wiedzy (m.in. dzięki wykorzystaniu generatywnej sztucznej inteligencji). Postęp technologiczny doprowadził do spadku kosztów komunikowania się i transportu, wzrostu szybkości przenoszenia się informacji oraz do stworzenia nowych produktów i usług (np. streamingu, smartfonów, otwartej bankowości, DeFi – *Decentralized Finance*, itp.). Przyczyniło się to z kolei do intensyfikacji istniejących już powiązań gospodarczych i technologicznych między krajami.

Globalizacja jest zjawiskiem wielowymiarowym, które polega na integrowaniu się – prowadzonej w skali międzynarodowej – działalności ekonomicznej gospodarstw domowych, przedsiębiorstw i banków krajowych i transnarodowych, sektorów i rynków oraz gospodarek narodowych. Są one podmiotami uczestniczącymi w procesie globalizacji, ale obok nich należy także wymienić podmioty o działaniu ponadnarodowym, tj. międzynarodowe ugrupowania integracyjne i międzynarodowe organizacje gospodarcze. W rezultacie globalizacji powstają nowe, bardziej intensywne powiązania gospodarcze oraz międzynarodowe współzależności (ang. *interdependencies*) pomiędzy przedsiębiorstwami, bankami i instytucjami finansowymi, poszczególnymi sektorami gospodarki, państwami, organizacjami międzynarodowymi. Charakterystyczne jest, że charakter tych powiązań i ich rezultaty nie zawsze (a w zasadzie na ogół) są symetryczne pod względem korzyści dla różnych stron.

Można zatem przyjąć, iż to właśnie negatywne aspekty globalizacji uwypukliły i wzmocniły oddziaływanie ryzyk geopolitycznych na sferę gospodarczą w skali całego świata. W tej sytuacji to właśnie szukanie przewag konkurencyjnych, wykorzystywanie sytuacji geopolitycznej, unikanie lub obniżanie ryzyka geopolitycznego stają się głównymi obszarami działań przedsiębiorstw, banków i rządów państw. Jest to przy tym bardzo trudne w warunkach ścisłych powiązań na wielu płaszczyznach. W oczywisty sposób rysuje się tu uprzywilejowanie pewnych głównych państw i podmiotów oraz trudniejsza pozycja mniejszych graczy, będących tylko *followersami* tendencji narzucanych przez „centrum" i państwa/podmioty hegemoniczne.

Charakterystyczne jest, że w ostatnich latach w gospodarce światowej zarysowały się tendencje deglobalizacyjne (Bello, 2004; Goldberg i Reed, 2023). Nie pretendując do dokładnego omówienia przyczyn takiego stanu rzeczy, należy wskazać, że z jednej strony był on następstwem zarówno wydarzeń losowych, mających znamiona „czarnych łabędzi" takich jak pandemia COVID-19, agresja Rosji na Ukrainę i jej konsekwencje, nasilenie konfliktów na Bliskim Wschodzie, czy napięcia na linii USA-Chiny, a z drugiej – procesów zachodzących w poszczególnych państwach i gospodarce światowej, głęboko uderzających w istniejące struktury rynkowe, instytucje oraz mechanizmy gospodarcze.

Procesy te mają dość ogólny, szeroki charakter, dalece wykraczający swoim znaczeniem i doniosłością poza geopolitykę, politykę gospodarczą czy funkcjonowanie poszczególnych rynków i branż (w tym systemu bankowego). Można je przy tym traktować jako czynniki wzrostu niepewności i ryzyka (w tym geopolitycznego) w gospodarce światowej. Jednocześnie, procesy te akcentują znaczenie poszczególnych wymiarów geopolityki i są przyczynkiem do nasilonych analiz w tym zakresie.

Z uwagi na znaczenie tych procesów, jak i bardzo szeroki zakres ich oddziaływania, określa się je mianem **„megatrendów"** (Diamandis i Kotler 2021). Znamienne jest przy tym, że najczęściej rozpatruje się je w kategoriach potencjalnych zagrożeń dla stabilności finansowej, gospodarczej i politycznej. Przykładowo, Roubini (2023), w nieco innym kontekście używa tu wręcz określenia „megazagrożenia" (ang. *megathreats*), rozumiejąc przez nie ogólne wyzwania o charakterze gospodarczym, finansowym, politycznym, geopolitycznym, branżowym, technologicznym, zdrowotnym czy klimatycznym. Autor ten analizuje 10 bardziej szczegółowych megazagrożeń, a mianowicie: (1) rosnące zadłużenie; (2) kryzysy finansowe i niestabilność zadłużenia; (3) pułapka łatwego pieniądza; (4) deglobalizacja; (5) niewydolność publiczna i prywatna; (6) problemy demograficzne; (7) zagrożenie ze strony AI; (8) nowa zimna wojna; (9) problemy klimatyczne oraz (10) stagflacja.

17 Pierwsza rewolucja przemysłowa wiązana była przede wszystkim z maszyną parową (umownie lata 1760–1900), wyróżnikiem drugiej były natomiast przede wszystkim silnik spalinowy i elektryczność (1900–1960). Otwartą jest natomiast kwestia, czy możemy mówić już o piątej rewolucji przemysłowej, wiązanej przede wszystkim ze sztuczną inteligencją i biologią syntetyczną.

Z kolei Tooze (2022) pisze o zjawisku tzw. **polikryzysów** (ang. *policrises*), stanowiących ogromne wyzwanie, przed jakimi stoją współcześni decydenci. Sam termin „polikryzys" wprowadzili już w 1999 r. Edgar Morin i Anne Kern, wykorzystując go do opisu sytuacji, w której problem stojący przed decydentami nie jest tylko jednym zagrożeniem, lecz stanowi całą złożoną współzależność problemów, antagonizmów, kryzysów, procesów wymykających się spod kontroli oraz ogólnego kryzysu dotykającego całą planetę[18]. Jak ujmuje to Tooze (2022): „problem staje się kryzysem, gdy podważa naszą zdolność do radzenia sobie, a tym samym zagraża naszej egzystencji/tożsamości. W przypadku polikryzysów wstrząsy są różnorodne, lecz oddziałują na siebie w taki sposób, że całość okazuje się jeszcze bardziej przytłaczająca niż suma jej części".

Zbliżoną koncepcją do polikryzysów jest tzw. permakryzys. Termin ten, zaproponowany przez byłego brytyjskiego premiera Gordona Browna, oznacza długi, utrzymujący się stan niepewności i niestabilności wynikający z niekończącej się sekwencji kryzysów. W odróżnieniu od pojedynczego, choćby bardzo dotkliwego kryzysu, permakryzys charakteryzuje się splątaniem wielu rozmaitych kryzysów – politycznych, gospodarczych, ekologicznych, społecznych – które wzajemnie się wzmacniają i utrudniają wyjście z sytuacji (zob. Brown i in., 2023).

Obie koncepcje — permakryzys i polikryzys — stanowią przykłady prób zrozumienia i objaśnienia współczesnych złożoności świata, które tworzą wiele różnego rodzaju wyzwań wzajemnie na siebie oddziałujących, wymagających różnorodnych odpowiedzi i wskazujących, że niczego nie można rozpatrywać w izolacji. Tym, co odróżnia permakryzys od polikryzysów jest trwałość (permanentność) występowania kryzysu mimo wspólnych wysiłków nadzorców, regulatorów i decydentów, skierowanych na łagodzenie konkretnych kryzysów w ściśle określonych obszarach (Mishra i Sen, 2024).

Zjawisko polikryzysów/permakryzysu ujawniło się w całej rozciągłości po wybuchu pandemii i wojny na Ukrainie, znamionując kres jednobiegunowego świata, świata „końca historii" (Fukuyama, 1992) czy „końca geografii" (Dodds, 2021). Odwróceniu uległy tendencje liberalizacyjne, globalizacyjne oraz integracyjne[19]. Pojawiły się ponownie bariery i utrudnienia w handlu, przepływach kapitałowych, a nawet w ruchu turystycznym – i to nie tylko między krajami wysokorozwiniętymi a słabiej rozwiniętymi, ale także w grupie samych najbogatszych państw świata. Te bariery przybierają znane od dawna formy (m.in. cła, większa kontrola przepływu osób pomiędzy państwami), ale też przybierają nowe formy (np. zamrażanie aktywów, wyłączanie z globalnego systemu płatności, restrykcje w obrocie metalami ziem rzadkich[20]). Co istotne, zwykle są one wprowadzane nagle, zwiększając skokowo niepewność i generując ryzyko dla wszystkich zaangażowanych podmiotów.

1.3. Ryzyko geopolityczne – definicje i sposoby pomiaru

Nasilenie debaty geopolitycznej i pogłębione analizy w tym obszarze nie są oczywiście celem samym w sobie. Finalnym rezultatem powinno być zrozumienie konsekwencji, jakie mogą nieść za sobą negatywne zdarzenia w zakresie opisywanych wymiarów geopolityki. W bezpośredni sposób sprowadza się to do zrozumienia i oszacowania ryzyka geopolitycznego, a także następstw jakie niesie ono z sobą.

Przez **ryzyko geopolityczne** (dalej: RGP) rozumie się zagrożenie dla prowadzenia działalności gospodarczej wynikające z geograficznej perspektywy związanej z powiązaniami z zagranicą i narażenia na skutki takich zdarzeń jak: wojna kinetyczna i zagrożenie wojną, konflikty, wojna handlowa, sankcje gospodarcze i polityczne, blokady szlaków transportowych i zagrożenie nimi, cyberataki, nielegalne migracje, polaryzacja sfery politycznej na świecie. Z kolei Caldara i Iacoviello (2022) utożsamiają ryzyko geopolityczne z „groźbą, realizacją i eskalacją niekorzystnych zdarzeń związanych z wojnami, terroryzmem i wszelkimi napięciami między państwami i podmiotami

18 "Complex intersolidarity of problems, antagonisms, crises, uncontrollable processes, and the general crisis of the planet" (Morin i Kern, 1999, s. 74).

19 Nie należy jednak mówić o końcu globalizacji, gdyż ona się nie kończy, ale raczej zmienia z powodu silnej współzależności w międzynarodowych łańcuchach dostaw. Tej współzależności nie sposób zastąpić w krótkim okresie lokalną (krajową) produkcją, a być może – zwłaszcza ze względów ekonomicznych, ale także z uwagi na globalną naturę osiągnięć technologicznych – nie da się tego zrobić także w dłuższym horyzoncie czasowym. Siła przedsiębiorstw globalnych jest tak duża, że mimo napięć i wojen handlowych, ceł i taryf nakładanych nagle przez liderów państw, szukają one nowych możliwości, zawiązują wciąż nowe współprace z innymi partnerami.

20 Ograniczenie takie wprowadziły Chiny w październiku 2025 r., co wzbudziło szerokie kontrowersje i nerwowe reakcje partnerów gospodarczych.

politycznymi, które wpływają na pokojowy przebieg stosunków międzynarodowych".

Ryzyko geopolityczne oznacza zatem nie tylko samo potencjalne zagrożenie wystąpienia problemów w innych krajach, rzutujących na sytuację krajową, ale może też skutkować faktycznym wystąpieniem danego wydarzenia – materializacją ryzyka. Jest ono również powiązane z innymi rodzajami ryzyka, często stanowiąc ich swoisty wyzwalacz (ang. *trigger*). Ryzyko geopolityczne jest przy tym bardzo trudne do wyizolowania, oddziałuje bowiem z jednej strony na wszelkie formy prowadzenia działalności gospodarczej, zarządzanie przedsiębiorstwami finansowymi i niefinansowymi oraz ich efektywność na poziomie mikro, z drugiej zaś rzutuje na sytuację makroekonomiczną i pozycję konkurencyjną całej gospodarki.

Z uwagi na przedmiot rozważań, w niniejszym opracowaniu rozważana będzie głównie płaszczyzna mikro. W tym kontekście, brytyjsko-amerykańska korporacja ubezpieczeniowa Willis Towers Watson (2019) określa ryzyko geopolityczne jako „numer 1 globalnego ryzyka korporacyjnego" (*number one global corporate risk*). Podkreśla się, że transmisja ryzyka geopolitycznego, o czym będzie jeszcze mowa w następnych sekcjach, następuje poprzez różnorodne kanały: handlu zagranicznego, łańcuchów wartości, przepływów kapitałowych, rynków finansowych i rynków towarów (ang. *commodities*). **Już tutaj warto nadmienić, że w odniesieniu do banków kanały, jakimi przenosi się ryzyko geopolityczne są liczne, złożone, wiążąc się przy tym z samą istotą działalności oraz z innymi rodzajami ryzyka bankowego**[21].

Ryzyko geopolityczne, gdy tylko się zmaterializuje, może istotnie wpłynąć na działalność wszelkich podmiotów: przedsiębiorstw (produkcyjnych, handlowych, usługowych), instytucji finansowych, a w tym oczywiście i banków, a także inwestorów (zwłaszcza nieprzygotowanych). Wpływ ten następuje poprzez wzrost kosztów, utratę pracowników, ograniczenia w handlu międzynarodowym (z powodu barier handlowych czy sankcji), odcięcie całego rynku, mogącego stanowić źródło znaczących profitów (np. sankcje na Rosję), panikę wśród akcjonariuszy, nagłe zaostrzenie regulacji, itp.

Na ryzyko geopolityczne narażone są w – sposób bezpośredni lub pośredni – wszystkie przedsiębiorstwa. Bezpośrednio narażone są na nie przedsiębiorstwa niefinansowe (produkcyjne, usługowe) i finansowe działające na rynku międzynarodowym, powiązane handlowo lub kapitałowo z innymi krajami. W przypadku przedsiębiorstw niefinansowych, prowadzą one handel produktami finalnymi i pośrednimi (zajmują miejsce w tworzeniu łańcucha własności). Ponadto są one też powiązane kapitałowo z innymi rynkami, pozyskując kapitał na innych rynkach niż tam, gdzie zarejestrowana jest spółka-matka. Powiązania kapitałowe dotyczą banków, instytucji finansowych i ubezpieczeniowych, które pozyskują i inwestują kapitał, udzielają kredytów w różnych krajach. Pośrednio narażone są na ryzyko geopolityczne przedsiębiorstwa działające tylko na rynku krajowym, których efektywność zależy jednak od kosztów surowców energetycznych, czy kosztów importowanych płodów rolnych oraz te, które oferują swoje usługi (np. bankowe, finansowe, technologiczne) innym przedsiębiorstwom z silną ekspozycją międzynarodową[22].

Pomiar ryzyka geopolitycznego, z uwagi na mnogość definicji oraz stosowanie często nieostrych, nie do końca zdefiniowanych pojęć, jest utrudniony. Ponadto może on zawierać dużą dozę komponentu subiektywnego w zależności od autorów lub instytucji przygotowujących mierniki ryzyka. Niemniej jednak, można wyróżnić kilka głównych, często wykorzystywanych w raportach i artykułach naukowych mierników, których podstawy metodologiczne nie budzą większych zastrzeżeń. Są to przede wszystkim:

- **indeks niepewności polityki gospodarczej** (*Economic Policy Uncertainty Index*), opracowany przez S. Bakera, N. Blooma oraz S. Davisa (Baker i in., 2016);
- **indeks ryzyka geopolitycznego** (GRI, *Geopolitical Risk Index*), opracowany D. Caldarę oraz M. Iacoviellego (Caldara i Iacoviello, 2022);
- **indeks ryzyka politycznego dla firm** (*Firm-Level Political Risk Index*), opracowany przez T. Hassana, S. Hollandera, L. van Lenta oraz A. Tahouna (Hassan i in., 2019).

Ponadto, pośrednio do szacowania ryzyka geopolitycznego wykorzystuje się także bazy danych takie jak:

- **Globalna Baza Danych Geopolitycznych i Medialnych** (oryg. Global Database of Events, Language, and Tone[23]);

21 Kwestie te stanowią przedmiot rozważań w części drugiej.

22 Wpływ ryzyka geopolitycznego na polski system bankowy będzie przedmiotem rozważań w osobnej sekcji.

23 https://www.gdeltproject.org/

- **Międzynarodowa Baza Danych Kryzysów Politycznych** (oryg. *The International Crisis Behavior*[24]).

Indeks ryzyka geopolitycznego, opracowany przez Caldarę i Iacoviellego jako modyfikacja indeksu niepewności polityki gospodarczej Bakera, Blooma i Davisa, zbudowano na podstawie występowania określeń sugerujących wzrost napięcia międzynarodowego w artykułach prasowych z wybranych 10 gazet („Chicago Tribune", „Daily Telegraph", „Financial Times", „The Globe and Mail", „The Guardian", „The Los Angeles Times", „The New York Times", „USA Today", „The Wall Street Journal" oraz „The Washington Post"). Indeks ten zawiera dane dla całego świata, dla wybranych krajów opracowywane są sub indeksy, a zakres czasowy obejmuje okres począwszy od 1900 po dzień dzisiejszy (bieżąca aktualizacja); indeks jest aktualizowany na początku każdego miesiąca.

Indeks Ryzyka Politycznego dla Firm konstruuje się z kolei na podstawie komunikatów (ang. *earning calls*) amerykańskich firm notowanych na giełdzie. Indeks ten także budowany jest na podstawie częstości występowania określeń związanych z ryzykiem politycznym, zawiera dane dla lat 2002–2021 i obecnie nie jest aktualizowany.

Globalna Baza Danych Geopolitycznych i Medialnych wykorzystując automatyczne przetwarzanie języka naturalnego, monitoruje wiadomości z całego świata w ponad 100 językach. Jest to największa tego typu baza na świecie; zawiera szczegółowe dane od 1979 roku do chwili obecnej i jest aktualizowana co 15 minut. Nie jest to zatem bezpośredni sposób pomiaru ryzyka geopolitycznego, ale może stanowić bezcenne źródło danych do monitorowania bieżącej sytuacji.

Międzynarodowa Baza Danych Kryzysów Politycznych obejmuje szczegółowy opis 512 kryzysów politycznych i geopolitycznych, które wydarzyły się w latach 1918–2021. Baza ta zawiera informacje o stronach uczestniczących w sporach, ich sile politycznej lub militarnej, reakcji społeczności międzynarodowej i lokalnej, a także dokładny opis przyczyn, przebiegu i skutków konfliktów. Baza ta nie jest źródłem pomiaru ryzyka geopolitycznego, ale dostarcza szczegółowych danych na temat przeszłych konfliktów i może być wykorzystywana w analizach typu *event-study*.

Z uwagi na cel raportu, do dalszej, pogłębionej analizy wykorzystany zostanie rozszerzony **indeks ryzyka geopolitycznego** (GPR). Tworząc indeks, autorzy przyjęli, iż ryzyko geopolityczne obejmuje zagrożenia, realizację oraz eskalację wydarzeń związanych z wojnami, terroryzmem oraz napięciami między państwami i aktorami politycznymi. Co istotne, podejście to obejmuje nie tylko zdarzenia faktyczne, ale także percepcję zagrożeń, co pozwala na ujęcie szerokiego spektrum napięć międzynarodowych.

Indeks GPR jest, jak wspomniano, zbudowany na podstawie analizy treści artykułów prasowych publikowanych w najważniejszych gazetach anglojęzycznych od 1900 r. W każdym miesiącu obliczany jest udział artykułów zawierających określone frazy związane z ryzykiem geopolitycznym (takie jak wojna, terroryzm, atom/atomowy, atak, zagrożenie, eskalacja i inne) w całkowitej liczbie publikacji. Indeks GPR dzieli się na komponenty: zagrożeń (*Geopolitical Threats Index* – GPT) oraz faktycznych zdarzeń (*Geopolitical Acts Index* – GPA), co pozwala na bardziej szczegółową analizę źródeł ryzyka. Dodatkowo utworzono 44 indeksy krajowe, mierzące ryzyko geopolityczne z perspektywy danego państwa.

Zastosowanie indeksu GPR pozwala na identyfikację wpływu ryzyka geopolitycznego na sytuację makroekonomiczną (w tym na podstawowe kategorie i makroagregaty, takie jak tempo wzrostu gospodarczego, poziom inwestycji, zatrudnienie, bezrobocie). Wyższe wartości indeksu są skorelowane z większym prawdopodobieństwem wystąpienia kryzysów gospodarczych, a także z obniżeniem poziomu inwestycji w sektorach szczególnie narażonych na ryzyko geopolityczne. Do takich sektorów należą m.in.: przemysł obronny, sektor naftowy i energetyczny, przemysł wydobywczy. Również sektor bankowy jest narażony na wzrost ryzyka geopolitycznego, który może skutkować zwiększeniem podatności na szoki zewnętrzne oraz trudnościami w międzynarodowej dywersyfikacji ryzyka (zob. np. Alsadan i in., 2025).

Na wykresach 1–2 zaprezentowano zmiany indeksu ryzyka geopolitycznego w czasie, od momentu wyjściowego, tj. 1900 r. Wartość 100 oznacza poziom ryzyka w styczniu 2019 r.

Na Wykresie 1. przedstawiono zmiany globalnego indeksu ryzyka geopolitycznego (GPR) w latach 1900–2025. Indeks ten opiera się, jak wspominano, na analizie treści artykułów prasowych z wiodących gazet anglojęzycznych. Z jednej strony pozwala to na kontrolę zmian i porównania w bardzo dłu-

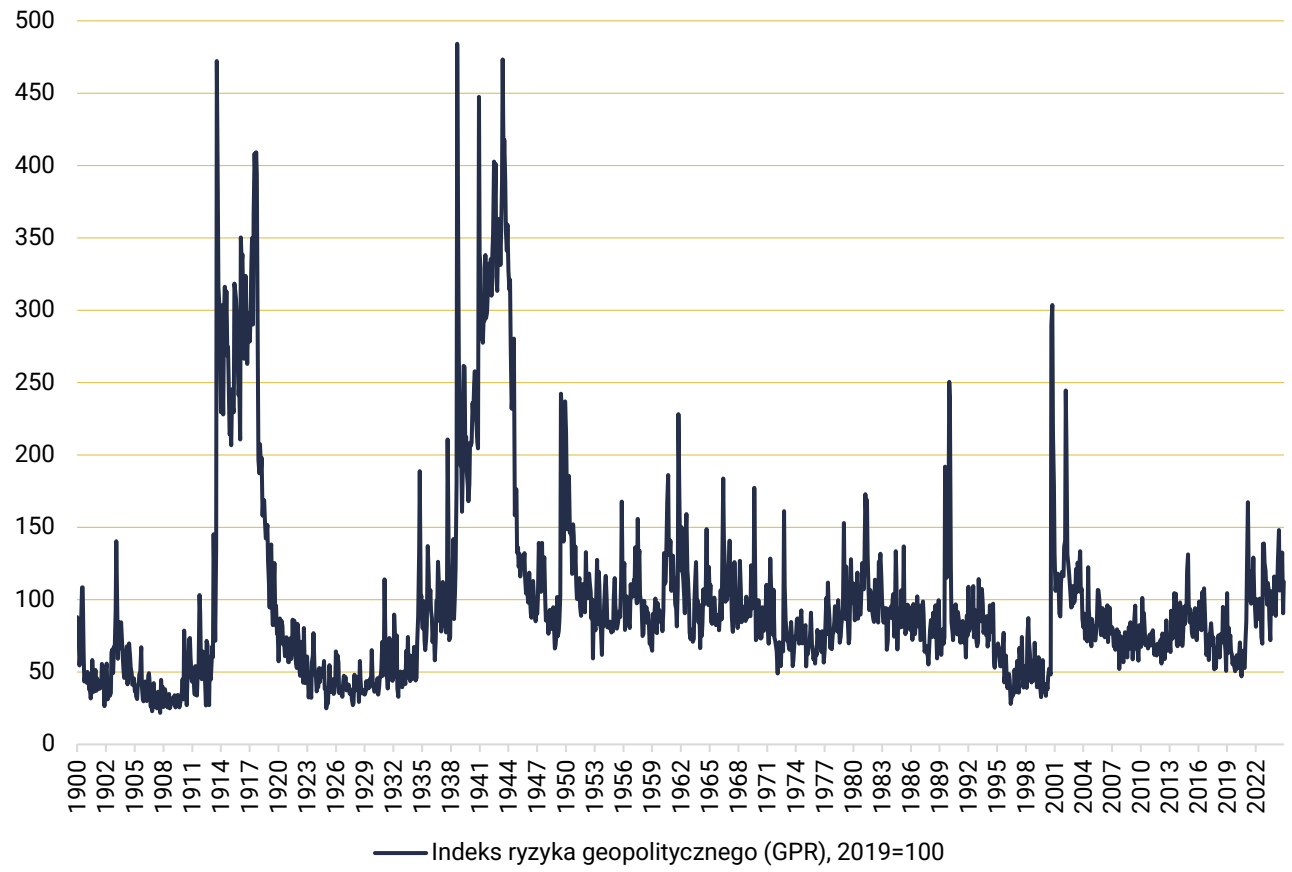
24 https://sites.duke.edu/icbdata/

gim horyzoncie czasowym, ale z drugiej – może w pewnym stopniu nadreprezentować perspektywę amerykańską i europejską[25]. Wartości indeksu zależą zarówno od rzeczywistych zdarzeń (wojny tzw. kinetyczne („gorące"), ataki terrorystyczne, zamachy stanu), jak i percepcji zagrożeń (retoryka polityczna, napięcia międzynarodowe). Na wykresie widoczne są wyraźne, dynamiczne wzrosty wartości indeksu w okresach największych globalnych napięć, w tym przede wszystkim w okresie pierwszej (1914–1918) i drugiej (1939–1945) wojny światowej, kryzysu kubańskiego (1962), ataków z 11 września 2001 roku oraz inwazji Rosji na Ukrainę w 2022 roku. W ostatnich latach zauważalny jest także wzrost ryzyka związany z napięciami wokół Tajwanu oraz eskalacją konfliktów na Bliskim Wschodzie. Warto podkreślić, że indeks reaguje nie tylko na faktyczne działania militarne, ale również na wzrost napięcia i niepewności geopolitycznej.

Na Wykresie 2. zaprezentowano natomiast rozkład indeksu GPR na komponent zagrożeń (GPT) oraz faktycznych zdarzeń (GPA). Dzięki temu możliwa jest bardziej precyzyjna analiza źródeł ryzyka. Widać, że w wielu przypadkach wzrost percepcji zagrożeń (GPT) wyprzedza wystąpienie faktycznych wydarzeń (GPA), co może świadczyć o roli mediów i oczekiwań społecznych w kształtowaniu nastrojów. Przykładem może być okres zimnej wojny, kiedy to GPT utrzymywał się na wysokim poziomie mimo braku bezpośrednich działań zbrojnych między mocarstwami.

Oba wykresy potwierdzają, że ryzyko geopolityczne ma charakter permanentny, cykliczny i silnie reaguje na zmiany w globalnym układzie sił. Wzrost wartości indeksu GPR może mieć istotne konsekwencje dla gospodarki – wpływa na poziom inwestycji, zatrudnienie oraz stabilność sektora finansowego. Dlatego monitorowanie tego wskaźnika jest istotne zarówno dla decydentów politycznych, jak i inwestorów.

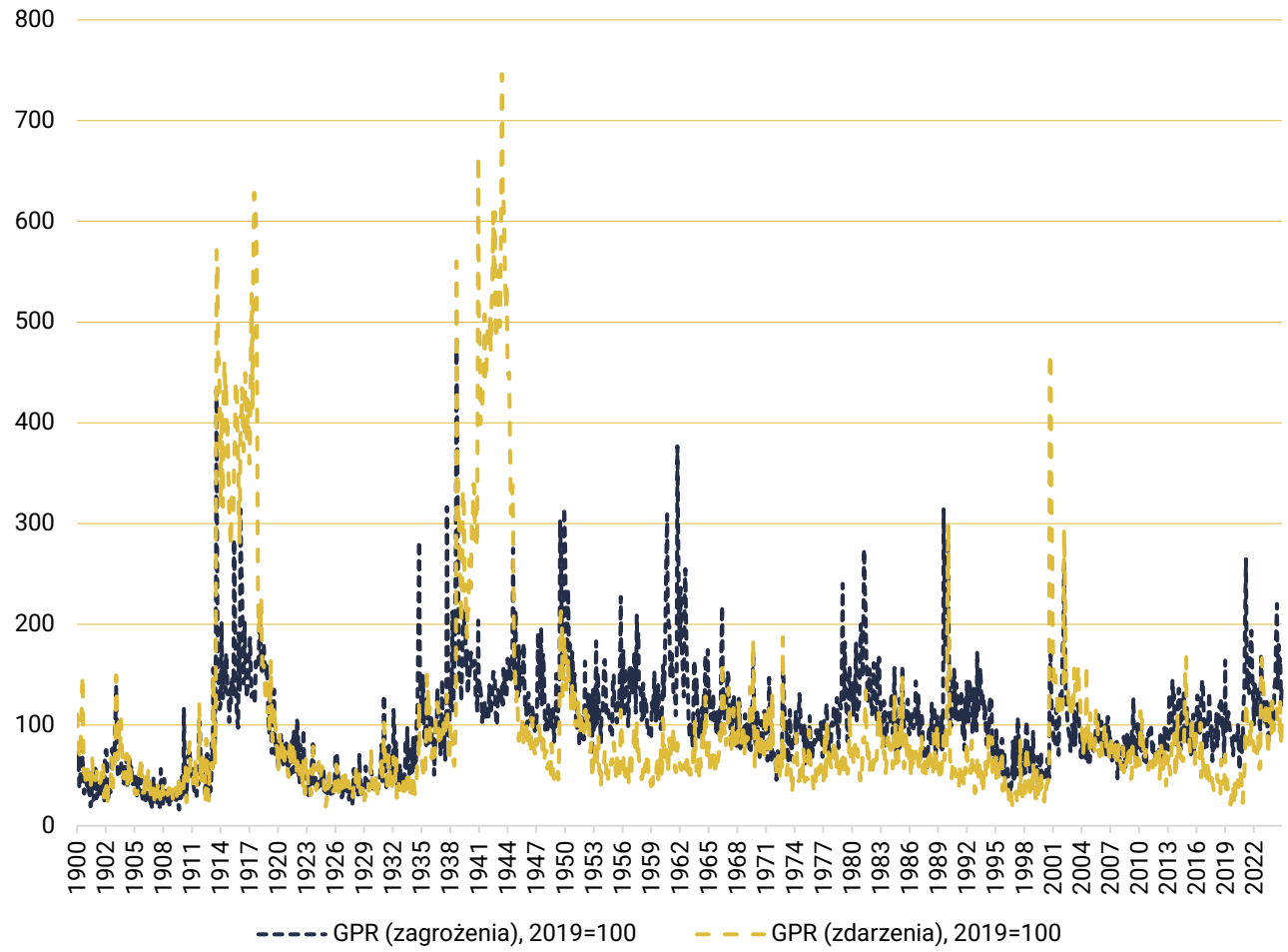
Wykres 1. Ryzyko geopolityczne na świecie w latach 1900–2025



Źródło: Opracowanie własne na podstawie Geopolitical Risk Index.

25 Należy zauważyć, że ten swoisty „westernocentryzm" wśród autorów anglosaskich i europejskich jest typowy, nie tylko w kwestii ryzyka geopolitycznego, ale całego postrzegania stosunków ekonomicznych, szacowania potencjału czy nawet interpretowania historii gospodarczej – w tym historii finansów i bankowości. Kwestie te poruszał np. Peter Frankopan (2025). Niewątpliwie utrudnia to obiektywne oceny zarówno sytuacji geopolitycznej, jak i ryzyka geopolitycznego. Z drugiej strony – trudno takiemu podejściu się dziwić.

Wykres 2. Komponenty indeksu ryzyka geopolitycznego na świecie w latach 1900-2025



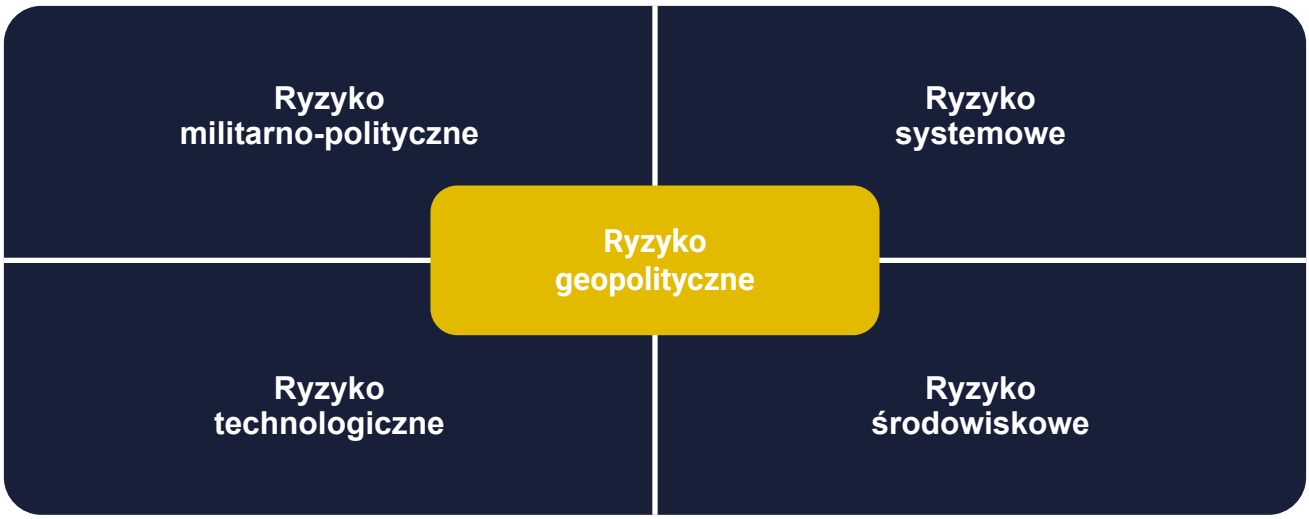
Źródło: Opracowanie własne na podstawie Geopolitical Risk Index.

Kończąc rozważania na temat kształtowania się oraz identyfikacji ryzyka geopolitycznego, należy uznać, iż monitorowanie indeksu GPR w ujęciu krajowym, a także w ujęciu rozmaitych przedziałów czasowych jest bardzo przydatne. Pozwala bowiem lepiej zrozumieć wpływ wydarzeń międzynarodowych na sytuację wewnętrzną, a także wspiera podejmowanie decyzji w zakresie polityki bezpieczeństwa, inwestycji zagranicznych i zarządzania ryzykiem. Rozpoznanie potencjalnych zagrożeń i uświadomienie sobie skali oraz źródeł ryzyka jest pierwszym krokiem w podjęciu adekwatnych i skutecznych działań mających je neutralizować.

1.4. Klasyfikacja źródeł i rodzajów współczesnego ryzyka geopolitycznego

Współczesne ryzyko geopolityczne przybiera coraz bardziej złożone i wielowymiarowe formy, wykraczające poza tradycyjne konflikty zbrojne. Wiodące instytucje analityczne, takie jak KPMG (2025), S&P Global (2025) oraz World Economic Forum (2025), wskazują na konieczność klasyfikacji ryzyk według ich charakteru, źródeł oraz wpływu na systemy polityczne, gospodarcze i społeczne. Na Rysunku 2. przedstawiono najważniejsze typy (odmiany) ryzyka geopolitycznego, wyodrębnione na podstawie ich źródeł. Charakterystyczne jest, że każda grupa obejmuje kilka specyficznych zagrożeń, generujących inny łańcuch przyczynowo-skutkowy następstw dla podmiotów finansowych i niefinansowych. Można też zauważyć, że korespondują one niejako z przedstawionymi w poprzedniej sekcji wymiarami geopolityki oraz elementami bieżącej agendy geopolitycznej. Przyporządkowanie danego rodzaju ryzyka do określonej grupy jest przy tym dość arbitralne; niektóre z nich mają charakter dość złożony, łącząc, przykładowo, elementy systemowe ze środowiskowymi.

Rysunek 2. Typy ryzyk geopolitycznych ze względu na ich źródła



Źródło: Opracowanie własne.

Do grupy ryzyk o **charakterze militarnym i politycznym** można zaliczyć: (1) „tektoniczne" przesunięcia sił; (2) zbrojne konflikty oraz tzw. wojny zastępcze (ang. *proxy wars*) oraz (3) zakłócenia w funkcjonowaniu łańcuchów dostaw. „Tektoniczne" przesunięcia w układzie sił odnoszą się do fundamentalnych zmian w globalnym układzie sił politycznych i gospodarczych. Obejmują one zmiany w dominacji geopolitycznej, powstawanie nowych bloków handlowych oraz wzrost znaczenia państw rozwijających się (np. Indie, Brazylia, państwa ASEAN, grupa BRICS). Przykładem tej grupy czynników są napięcia handlowe między USA a Chinami, które prowadzą do przekształcenia globalnych łańcuchów wartości i redefinicji sojuszy strategicznych[26]. Ryzyko to może skutkować mniejszą sprawczością instytucji międzynarodowych oraz wzrostem protekcjonizmu gospodarczego. Zbrojne konflikty i wojny zastępcze obejmują konflikty międzypaństwowe, wojny domowe, zamachy stanu oraz wzrost siły i znaczenia ugrupowań terrorystycznych (wojna asymetryczna). Zdarzenia te występują w ograniczonej liczbie (szczególnie w porównaniu do innych typów ryzyka geopolitycznego), ale ich wpływ na stabilność globalną jest ogromny. Przykładem ryzyka geopolitycznego zaliczanego do tej grupy są wojna w Ukrainie, konflikty w Syrii, Jemenie, czy regionie Sahelu, ale też działalność piratów na Morzu Czerwonym. Często są one powiązane z rywalizacją mocarstw i mają charakter wzmiankowanych wojen zastępczych, w których lokalne konflikty są determinowane przez zewnętrzne siły[27]. Konflikty tego typu, ale także następstwa zmian klimatycznych, protekcjonizm i cyberataki zakłócają efektywne funkcjonowanie globalnych łańcuchów dostaw. Na konsekwencje są szczególnie narażone sektory strategiczne, m.in. energetyka, żywność, farmaceutyki i technologie. Przykładem są zakłócenia transportu przez Kanał Sueski, blokady cieśniny Ormuz, konieczność zmiany tras samolotów transportowych zmuszonych do omijania rejonów objętych działaniami militarnymi, napięcia wokół Tajwanu czy ograniczenia eksportowe surowców krytycznych.

Drugą grupę stanowią **ryzyka o podłożu systemowym**. Coraz częściej – szczególnie w zglobalizowanym świecie – podkreśla się konsekwencje tzw. fragmentaryzacji regulacyjnej. Proliferacja niespójnych regulacji i polityk podatkowych między państwami[28] prowadzi do trudności w prowadzeniu działalności międzynarodowej, transgranicznej, zaburza działanie mechanizmu rynkowego, a także umożliwia uzyskiwanie nieuczciwej przewagi konkurencyjnej niewynikającej z wydajności produkcji czy stosowanej technologii. Fragmentacja ta zwiększa koszty, potencjalnie ogranicza napływ bezpośrednich inwestycji zagranicznych oraz sprzyja powstawaniu dodatkowych barier pozataryfowych w handlu. Kolejnym typem ryzyka o charakterze systemowym jest wspominana w poprzedniej sekcji **deglobali-**

26 Często używa się tu określenia „pułapka Tukidydesa", nawiązującego do nieuchronnej konfrontacji dotychczasowego hegemona ze wschodząca potęgą (ang. *challenger*). (Allison, 2016). Sam Tukidydes pisał o tym w kontekście wojny peloponeskiej Aten ze Spartami.

27 Nie jest to oczywiście novum. Znamiona proxy war miały również konflikt wietnamski czy afgański.

28 Przykładem są różnice w podejściu do opodatkowania gospodarki cyfrowej, wdrażania globalnego podatku minimalnego czy regulacji dotyczących danych osobowych. Jak się wydaje, podobny charakter mogą mieć także regulacje odnośnie do skali i zasad wykorzystywania sztucznej inteligencji.

zacja. Najogólniej, można ją rozumieć jako proces polegający na zahamowaniu, spowolnieniu lub nawet odwróceniu dotychczasowych trendów integracji gospodarczej, politycznej i technologicznej między państwami. W przeciwieństwie do globalizacji, opierającej się na swobodnym przepływie towarów, kapitału, ludzi i informacji, deglobalizacja jest tożsama ze wzrostem barier handlowych, nasileniem protekcjonizmu czy wręcz nacjonalizmem gospodarczym oraz ograniczeniem współpracy międzynarodowej. Przykładem może być opuszczenie struktur Unii Europejskiej przez Wielką Brytanię (*Brexit*), powracające napięcia handlowe pomiędzy USA a Chinami oraz ograniczanie eksportu wybranych surowców, produktów (np. półprzewodników) lub technologii (w tym głównie o wysokim znaczeniu militarnym). Do grupy ryzyka systemowego można także zaliczyć wojny walutowe (między innymi kwestie świadomej dewaluacji dolara przez USA, chiński dumping kursowy) oraz działania na rzecz osłabienia statusu dolara jako globalnej waluty rezerwowej, utożsamiane z dążeniem do tzw. dedolaryzacji dolara, a w perspektywie być może z całkowitą przebudową globalnego systemu monetarnego.

Trzecia odmiana ryzyka geopolitycznego obejmuje **ryzyka technologiczne**. Rozpatrywanymi tu kwestiami są cyberataki i problemy z cyberbezpieczeństwem, zarówno dla agend i instytucji rządowych, jak i podmiotów gospodarczych oraz nawet osób fizycznych (np. destabilizacja systemów płatniczych i transakcyjnych), działalność grup APT (*Advanced Persistent Threat*), wykorzystywanie nowoczesnych technologii do wywierania wpływu na wyniki wyborów i kształtowania postaw społeczeństw, wykorzystywania nowoczesnych technologii (np. kryptowalut) do omijania sankcji międzynarodowych i/lub regulacji ostrożnościowych oraz procedur AML, itp. Z uwagi na bardzo bliskie związki z bezpieczeństwem i stabilnością systemów bankowych kwestie te będą przedstawione bardziej szczegółowo w kolejnej sekcji

Czwarta grupa zawiera **ryzyka o podłożu środowiskowym**. Jednym z nich są zmiany klimatu prowadzące do ekstremalnych zjawisk pogodowych, niedoboru zasobów naturalnych, migracji klimatycznej i napięć międzypaństwowych. Ryzyko to ma przy tym charakter systemowy i ponadnarodowy – wpływa bowiem na bezpieczeństwo żywnościowe, zdrowotne, ale także militarne. Przykładem są konflikty o wodę, susze w regionach rolniczych, wzrost liczby katastrof naturalnych oraz zwiększone tempo migracji z regionów o gorszych warunkach klimatycznych. Z czynnikami środowiskowymi nierozerwalnie związane jest także szerokorozumiane bezpieczeństwo energetyczne. Zależność od importu surowców energetycznych, konflikty w regionach wydobycia oraz cyfryzacja sektora energetycznego zwiększają podatność na zakłócenia. Przykładem są ataki (zarówno kinetyczne, jak i cyfrowe) na infrastrukturę energetyczną, manipulacje cenami surowców oraz geopolityczne napięcia wokół dostaw gazu i ropy naftowej. Transformacja energetyczna (np. odejście od paliw kopalnych) również generuje nowe ryzyka związane z dostępem do surowców krytycznych, w tym wykorzystywanych do produkcji urządzeń umożliwiających wykorzystywanie odnawialnych źródeł energii. Rozważania te w sposób syntetyczny podsumowano w Tabeli 1., podając przy tym obszary ich występowania w ostatnich latach.

Tabela 1. Klasyfikacja współczesnych typów ryzyka geopolitycznego

Grupa ryzyka	Typ ryzyka	Główne źródła	Przykłady/Obszary występowania
Militarno-polityczne	„Tektoniczne" przesunięcia sił	Zmiany sojuszy, polityka handlowa	USA–Chiny, Indo-Pacyfik
	Zbrojne konflikty i wojny zastępcze	Rywalizacja mocarstw, terroryzm	Ukraina, Bliski Wschód, Afryka Subsaharyjska
	Zagrożenia dla łańcuchów dostaw	Konflikty, klimat, protekcjonizm	Kanał Sueski, Tajwan, Arktyka, Cieśnina Ormuz
Systemowe	Fragmentacja regulacyjna	Brak harmonizacji przepisów	UE vs. reszta świata, podatki cyfrowe
	Deglobalizacja	Protekcjonizm, populizm, kryzysy globalne	Brexit, wojna handlowa USA–Chiny
	Wojny walutowe	Dążenie do osiągania korzyści ze słabszej waluty	Polityka USA, chińska polityka kursowa
	Dedolaryzacja	Dekonstrukcja światowego systemu monetarnego,	Działania krajów BRICS, bilateralne porozumienia dotyczące fakturowania i rozliczania handlu w walutach innych niż USD

Źródło: *Opracowanie własne.*

Grupa ryzyka	Typ ryzyka	Główne źródła	Przykłady/Obszary występowania
Technologiczne	Ryzyko technologiczne i cyfrowe	Cyberataki, AI, dezinformacja	Rosja, Chiny, USA
	Wojna cybernetyczna	Sabotaż, szpiegostwo, grupy hakerskie	Infrastruktura krytyczna, proces wyborczy, sektor energetyczny
Środowiskowe	Ryzyko klimatyczne	Ekstremalne zjawiska pogodowe, niedobory zasobów	Sahel, Azja Południowa, Ameryka Łacińska
	Bezpieczeństwo energetyczne	Konflikty, cyberataki, zmiany klimatu	Bliski Wschód, Rosja, Afryka

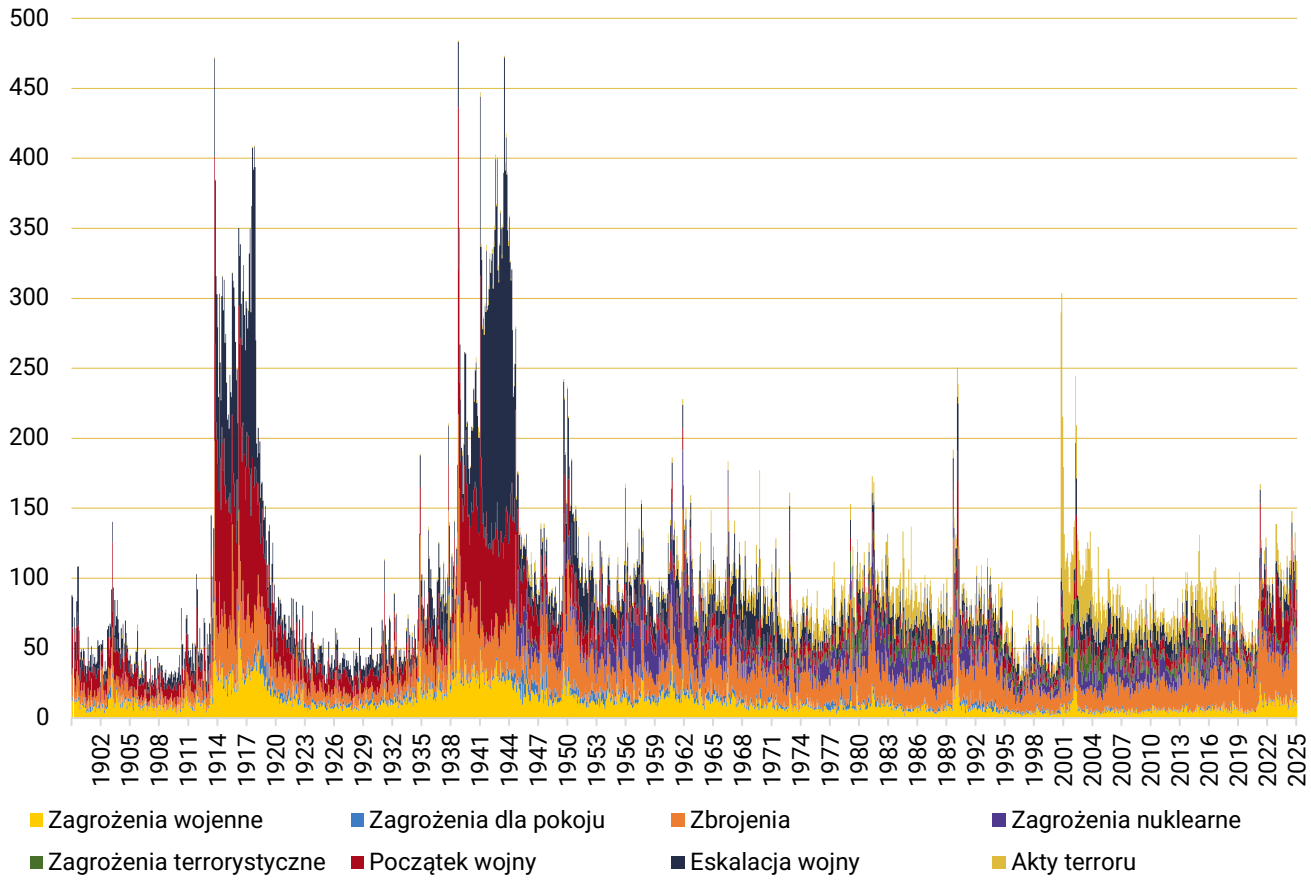
Źródło: *Opracowanie własne.*

1.5. Rozkład ryzyka geopolitycznego w czasie

Jak wynika z analizy źródeł rodzajów ryzyka geopolitycznego, jest ono niewątpliwie zjawiskiem bardzo złożonym. Odzwierciedla ono napięcia, konflikty i zagrożenia wynikające z relacji międzynarodowych, działań państw i aktorów niepaństwowych oraz globalnych procesów politycznych i militarnych. Właściwa percepcja i zrozumienie tego ryzyka są warunkami koniecznymi skutecznych działań poszczególnych podmiotów na rzecz ograniczania tego ryzyka bądź minimalizacji jego skutków. Z tego względu celowa i zasadna wydaje się być analiza rozkładu ryzyka geopolitycznego w czasie oraz struktury typów ryzyka. Pozwoli to lepiej zrozumieć ewolucję zagrożeń, z jakimi mierzy się społeczność międzynarodowa.

Na potrzeby tej analizy, bazując na danych z GRI, przygotowano dwa wykresy: Wykres 3 ukazuje ogólny poziom ryzyka w latach 1900–2025 z podziałem na poszczególne kategorie tego ryzyka, natomiast Wykres 4. ilustruje zmiany w rozkładzie jego poszczególnych typów.

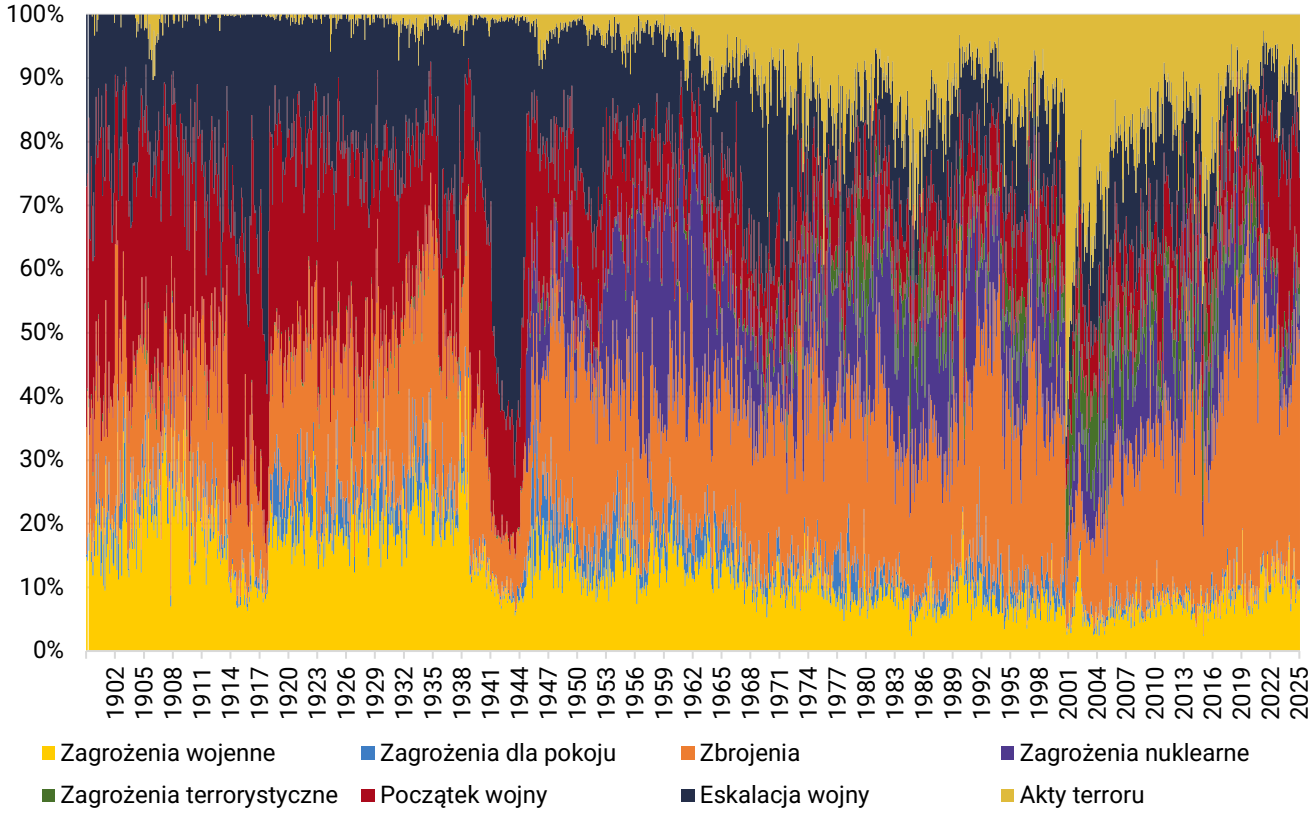
Wykres 3. Ryzyko geopolityczne na świecie w latach 1900-2025 (według kategorii ryzyka)



Źródło: *Opracowanie własne na podstawie Geopolitical Risk Index.*

W pierwszych dekadach XX wieku ryzyko geopolityczne było niemal całkowicie zdominowane przez klasyczne, kinetyczne konflikty zbrojne. Na Wykresie 3. można zaobserwować gwałtowne wzrosty indeksu w czasie I wojny światowej (1914–1918) oraz II wojny światowej (1939–1945), które były globalnymi konfliktami angażującymi większość ówczesnych mocarstw. W tym samym czasie, jak pokazano na Wykresie 4., struktura ryzyka była niemal jednowymiarowa – dominowały zagrożenia militarne; inne formy ryzyka były marginalne. Po 1945 r. świat wszedł w okres zimnej wojny, który przyniósł zmianę charakteru ryzyka geopolitycznego. Choć nie doszło do bezpośredniego, militarnego konfliktu między Stanami Zjednoczonymi a Związkiem Radzieckim, rywalizacja ideologiczna i militarna skutkowała utrzymywaniem się wysokiego poziomu napięć. Wykres 3. pokazuje liczne szczyty indeksu GPR w momentach kryzysów: wojny koreańskiej (1950–1953), kryzysu kubańskiego (1962), wojny w Wietnamie (szczególnie 1965–1973) czy radzieckiej interwencji w Afganistanie (1979–1989). W tym czasie rozkład ryzyka uległ znacznej dywersyfikacji – obok klasycznych wojen pojawiły się napięcia zimnowojenne oraz podwyższone ryzyko konfliktu nuklearnego, które w latach 60. i 70. ubiegłego wieku stanowiło istotny komponent globalnego zagrożenia.

Wykres 4. Rozkład typów ryzyka geopolitycznego na świecie w latach 1900-2025



Źródło: Opracowanie własne na podstawie Geopolitical Risk Index.

Upadek ZSRR w 1991 roku przyniósł krótkotrwałą stabilizację. Na Wykresie 3. można zaobserwować pewien spadek (malejącą amplitudę) indeksu GPR, co odzwierciedlało nadzieje na stabilizację, pokój i dominację liberalnego porządku międzynarodowego. Struktura ryzyka ulegała jednakże dalszemu rozproszeniu – pojawiły się nowe typy zagrożeń, takie jak konflikty etniczne, wojny domowe i niestabilność państw postkomunistycznych. Choć poziom ryzyka był globalnie niższy niż w okresie zimnej wojny, jego charakter stał się bardziej złożony i trudniejszy do przewidzenia. Przełom w rozkładzie ryzyka stanowią ataki na World Trade Center z 11 września 2001 roku, które radykalnie zmieniły percepcję zagrożeń. Przede wszystkim, znacząco i gwałtownie wzrósł ogólny poziom ryzyka geopolitycznego, a dodatkowo – co pokazano na Wykresie 4. – widać wyraźną dominację terroryzmu jako głównego typu ryzyka geopolitycznego. W kolejnych latach, mimo że poziom ryzyka nie osiągał już wartości z czasów wojen światowych, utrzymywał się on na podwyższonym poziomie z powodu licznych interwencji zbrojnych (Afganistan, Irak, Libia, Syria), zamachów terrorystycznych w Europie i Azji oraz wzrostu aktywności organizacji terrorystycznych takich jak Al-Kaida czy tzw. Państwo Islamskie.

W ostatnich latach obserwuje się ponowny wzrost ryzyka geopolitycznego, m.in. w związku z agresją Rosji na Ukrainę (2022), napięciami wokół Tajwanu, rywalizacją USA–Chiny oraz eskalacją konfliktów na Bliskim Wschodzie i w Afryce. Postępuje także dalsza dywersyfikacja struktury ryzyka – obok terroryzmu coraz większe znaczenie zyskują konflikty regionalne, nowy wyścig zbrojeń oraz kolejne wojny zastępcze (*proxy wars*).

Analiza obu wykresów pozwala dostrzec wyraźną ewolucję ryzyka geopolitycznego: od dominacji klasycznych wojen w pierwszej połowie XX wieku, przez napięcia zimnowojenne i ryzyko atomowe, aż po współczesne zagrożenia o charakterze asymetrycznym i hybrydowym, często zachodzące w domenie cybernetycznej. W konsekwencji, dzisiejsze ryzyko geopolityczne jest bardziej złożone, trudniejsze do przewidzenia. Stawia to niewątpliwie większe wymagania przed uczestnikami procesów politycznych i gry rynkowej oraz wymaga nowego podejścia do analizy oraz zarządzania bezpieczeństwem sektorowym i międzynarodowym. Jak się przy tym wydaje, wyraźniejszy niż w okresie „klasycznej" geopolityki jest obecnie wymiar ekonomiczny napięć geopolitycznych, a systemy finansowe, monetarne i płatnicze są płaszczyzną intensywnej rywalizacji. Oczywiście, posiadanie globalnej waluty rezerwowej czy ekspansja kapitału i instytucji finansowych zawsze były instrumentem wywierania wpływu i budowania dominacji. Można uznać, że w warunkach natężenia i przyspieszenia procesów finansyzacji gospodarki i życia społecznego, typowych dla końca ubiegłego i początków tego stulecia (Marszałek, 2014; Ratajczak, 2017), właśnie ten wymiar ryzyka geopolitycznego i czynniki z nim związane nabierają szczególnego znaczenia.

Część 2. Wybrane manifestacje ryzyka geopolitycznego w sferze monetarnej i finansowej

2.1. Wojny walutowe i „weaponizacja" walut

Jak wspominano, we współczesnej rywalizacji geopolitycznej instrumenty przymusu ekonomicznego wykorzystywane są nawet częściej niż tradycyjny nacisk militarny czy polityczny. Szczególnie przydatnymi narzędziami są tu rozmaite kategorie związane z pieniądzem i sferą monetarną.

Koncepcja wykorzystania narodowej waluty jako narzędzia budowania pozycji międzynarodowej danego państwa oczywiście nie stanowi novum. Ingerencję w dany narodowy system monetarny i płatniczy (np. fałszowanie pieniędzy i próby obniżania jego wartości) zawsze postrzegano jako próbę zdobycia kontroli lub co najmniej destabilizacji danego państwa[29]. Z drugiej strony, wzmacnianie pozycji własnej waluty, rozszerzanie przestrzeni monetarnej, na jakiej się nią posługiwano, oraz zachęcanie do posługiwania się w rozmaitych transakcjach rzeczowych i finansowych były naturalnym i logicznym sposobem budowania własnej przewagi[30].

Szczególne korzyści płyną oczywiście z faktu posiadania przez daną walutę narodową statusu **globalnej waluty rezerwowej**. Począwszy od lat 30. ubiegłego wieku pozycją taką cieszy się dolar amerykański (USD), który zastąpił w tej roli funta szterlinga. Niewątpliwie, był on jednym z filarów zbudowania mocarstwowej pozycji Stanów Zjednoczonych. Dobitnie uwypukliło się to w okresie funkcjonowania w latach 1944–1971 systemu dewizowo-złotego, zwanego potocznie systemem z Bretton Woods. System ten, mający charakter asymetryczny, był jednym z instrumentów budowania gospodarczej przewagi USA, których waluta była w tym systemie uprzywilejowaną, jako jedyny narodowy pieniądz wymienialny na złoto.

Posiadanie dominującej czy choćby stabilnej i silnej waluty, na którą zgłaszany jest duży popyt, otwiera szerokie perspektywy. Reglamentowanie jej podaży, wprowadzenie obowiązku rozliczeń w tej walucie czy możliwość kontroli uczestnictwa w światowych przepływach kapitałowych (w tym wykluczenie z nich jakiegoś kraju) stanowią skuteczne narzędzie nacisku. Z drugiej strony, działania takie spotykają się z reakcją innych państw, niechętnie spoglądających na przymus związany z posługiwaniem się określoną globalną walutą rezerwową, jak i na potencjalne ograniczenia, na jakie może napotkać ich aktywność ze strony hegemona monetarnego w przypadku wejścia z nim w konflikt czy choćby rywalizację.

Innym wymiarem wykorzystania pieniądza do rywalizacji geopolitycznej są tzw. **wojny walutowe**, czyli, najogólniej, granie na obniżkę wartości swojej waluty, by w ten sposób zwiększyć konkurencyjność eksportu danego kraju. Przykładami takiego procederu mogą być chociażby takie epizody jak „polityka zubażania" sąsiada (ang. *„beggar-thy-neighbor"*) z lat 30. ubiegłego wieku, słynne Plaza Accord z 1985 roku czy dewaluacje yuana z lat 2015–2016. Tego typu działalność ewidentnie zwiększa ryzyko geopolityczne w jego aspekcie systemowym. Oprócz poważnych konsekwencji makroekonomicznych, wojny walutowe w bezpośredni sposób wpływają też na instytucje finansowe, zagrażając bankom z ekspozycjami walutowymi.

Wszystkie te zjawiska można było, z różnym natężeniem, zaobserwować w ostatnich pięciu latach. I tak, w szczególności, można tu wskazać na następujące, „geopolityczne" wykorzystanie sfery monetarnej i finansowej:

1. **Weaponizacja dolara i systemu SWIFT (2022–2025)** Po inwazji Rosji na Ukrainę nastąpiła bezprecedensowe użycie narzędzi finansowych – zamrożenie rezerw walutowych Rosji[31] i wykluczenie ze SWIFT.

2. **Agresywna polityka wspierania juana (2023–2024)** – Chiny aktywnie promują internacjonalizację juana, szczególnie w handlu surowcami energetycznymi i umowach bilateralnych; co można interpretować jako „cichą" wojnę walutową

29 Warto tu przypomnieć choćby plany zdestabilizowania przez Niemcy gospodarki brytyjskiej za pomocą zalewu fałszywych funtów trakcie drugiej wojny światowej.

30 W tym kontekście ukuto koncepcję tzw. „pieniężnego Machiavellego", zgodnie z którą wojna walutowa i szukanie przewagi pieniężnej stanowią jeden z elementów strategii geopolitycznej i szukania zdobycia przewagi konkurencyjnej na arenie międzynarodowej.

31 Wcześniej podobne kroki zastosowano wobec Iranu w latach 2011–2016; skala tych działań była jednak zdecydowanie mniejsza.

i działania na rzecz obniżenia pozycji dolara jako waluty globalnej.

3. **Konkurencja w deprecjacji (2022–2023)** – podczas cyklu podwyżek stóp przez System Rezerwy Federalnej (SRF) silny dolar wywierał presję na inne banki centralne; szczególnie niekorzystne było to dla jena japońskiego, którego kurs spadł do najniższych poziomów od dekad, co wymusiło interwencję Banku Japonii.

4. **Działania i deklaracje monetarne BRICS** – porozumienia i umowy mające na celu ograniczenie roli dolara amerykańskiego w transakcjach i rozliczeniach; deklaracje (raczej niemożliwe w obecnych warunkach do urzeczywistnienia) o wprowadzeniu wspólnej waluty dla krajów tego ugrupowania.

Szczególnie interesująca jest tutaj pierwsza z wymienionych powyżej kwestii. Skupia się w niej bowiem cała złożoność geopolitycznego wykorzystania instrumentów finansowych i problemy, jakie przysparza to nie tylko tym, w których wymierzono cios, ale i tym, którzy danego narzędzia użyli. Z ryzykiem geopolitycznym muszą się tu bowiem mierzyć wszystkie strony, w tym także podmioty niezaangażowane bezpośrednio w główny konflikt. „Sankcyjne" zastosowanie globalnej waluty rezerwowej generuje efekty nie tylko w krótkim okresie (zazwyczaj korzystne dla kraju stosującego, czy ściślej rzecz ujmując, efekty zgodne z jego zamysłami), ale i długoterminowe, a głównym czynnikiem, który ma tu ostatecznie znaczenie, jest zaufanie.

Punktem wyjścia była tu podjęta w marcu 2022 roku przez państwa G7 i UE bezprecedensowa decyzja o zamrożeniu około 300 miliardów euro rezerw Centralnego Banku Rosji (utrzymywanych głównie w euro i dolarach). W dalszej kolejności podjęto kolejne, równie dotkliwe kroki: wykluczenie kluczowych rosyjskich banków ze SWIFT, wprowadzenie sankcji wtórnych wymuszających odpowiednie dostosowania podmiotów trzecich, które, same chcąc uniknąć sankcji, ograniczyły swoje transakcje z rosyjskimi firmami i instytucjami finansowymi, a także uniemożliwienie Rosji dostępu do międzynarodowych rynków kapitałowych.

Cel w postaci pogorszenia sytuacji Rosji i jej zdolności gospodarczych i finansowych został wprawdzie osiągnięty, niemniej działania te pociągnęły za sobą szereg poważnych reperkusji. Przede wszystkim, wywołały swoistą reakcję obronną nie tylko krajów nieprzyjaznych, ale wzbudziły też wątpliwości nawet wśród krajów neutralnych czy sojuszniczych. Oprócz spadku zaufania do dolara i władz amerykańskich, pojawiły się konkretne działania. Mianowicie, nastąpiło przyspieszenie prac nad alternatywnymi systemami rozliczeniowymi (CIPS – *China International Payment System* oraz rosyjski SPFS – *System for Transfer of Financial Messages*, pomyślane jako swoista alternatywa dla systemu SWIFT), a także nasiliły się sygnalizowane próby umów i sojuszy mających na celu działania w kierunku dedolaryzacji, a przynajmniej osłabienia pozycji waluty amerykańskiej, takie jak np. rozwój handlu dwustronnego w walutach lokalnych (Chiny-Rosja, Indie-Rosja)[32].

Na dłuższą metę wykorzystanie instrumentów monetarnych skutkuje zatem erozją zaufania do użytej dla osiągnięcia celów geopolitycznych waluty oraz generuje wyższe ryzyko geopolityczne. Ostatecznymi, długofalowymi konsekwencjami może być tu zjawisko tzw. fragmentacji monetarnej, a także „nowy" problem tzw. niemożliwej trójcy (ang. *impossible trinity 2.0*). O ile w pierwotnej koncepcji tego trylematu zakładano, iż możliwe jest osiągnięcie co najwyżej 2 z 3 celów: stałego kursu, swobodnego przepływu kapitału oraz niezależnej polityki monetarnej, to ta nowa koncepcja przenosi wybór na płaszczyznę relacji z USA jako hegemonem monetarnym. W tym ujęciu trylemat sprowadza się do tego, iż nie można mieć jednocześnie integracji z systemem dolarowym, suwerenności politycznej wobec USA oraz bezpieczeństwa rezerw walutowych.

Ostatecznie, rośnie ryzyko dla wszystkich podmiotów, w tym dla instytucji bankowych, konfrontowanych z różnymi rodzajami ryzyka, będącymi pochodną zawirowań w sferze monetarnej, wahań kursów walutowych, niestabilności politycznej, problemów kredytobiorców, których dotknęły sankcje monetarne, itp. (zob. szerzej część 4).

2.2. Cyberzagrożenia dla sektora finansowego

Obecną sytuację związaną z cyberzagrożeniami dla banków należy analizować z perspektywy całego sektora finansowego. Współczesne banki coraz rzadziej ograniczają się wyłącznie do tradycyjnych usług bankowych. Coraz więcej banków oferuje również usługi inwestycyjne, ubezpieczeniowe,

32 Osobnym, fascynującym nurtem jest tu wzrost zainteresowania powrotem do monetarnego wykorzystania złota.

a także, co szczególnie istotne z punktu widzenia cyberbezpieczeństwa, rozwiązania z zakresu technologii finansowych (FinTech). Taka różnorodność działalności sprawia, że analiza sytuacji banków wymaga uwzględnienia ich roli w kontekście szeroko rozumianego sektora finansowego[33].

Sektor finansowy każdego państwa odgrywa kluczową rolę w zapewnianiu stabilności i rozwoju gospodarki – jego niezakłócone funkcjonowanie jest niezbędne dla prawidłowego obiegu pieniądza i generalnej alokacji kapitału, efektywnych procesów oszczędzania, inwestowania oraz rozliczeń, a także codziennej działalności przedsiębiorstw i gospodarstw domowych. W związku z tym sektor finansowy, obok infrastruktury militarnej i krytycznej, może stanowić jeden z głównych celów cyberataków, motywowanych czynnikami geopolitycznymi. Dotyczy to zwłaszcza instytucji bankowych, których problemy, z uwagi na ich rolę w codziennym funkcjonowaniu obywateli, przedsiębiorstw czy innych instytucji, łącznie ze sferą rządową, w największym stopniu mogą zdestabilizować sytuację w danym państwie.

Złożoność usług finansowych oraz ich dostępność dla szerokiego grona użytkowników generują dodatkowe wyzwania w zakresie bezpieczeństwa. Usługi te najczęściej dostarcza się już z wykorzystaniem zaawansowanych technologii informacyjnych, co w połączeniu z różnym poziomem wiedzy i umiejętności użytkowników zwiększa ryzyko wystąpienia incydentów/zakłóceń w sprawnym funkcjonowaniu instytucji finansowych lub przebiegu poszczególnych transakcji. Instytucje te (a zwłaszcza banki) muszą zatem dbać nie tylko o aspekty technologiczne (częściowo przenoszone na klientów, np. bezpieczeństwo urządzeń mobilnych, sieci telekomunikacyjnych czy metod autoryzacji transakcji) oraz prawne, ale przede wszystkim o budowanie świadomości w zakresie cyberbezpieczeństwa. To właśnie postawa ludzi, zarówno pracowników, jak i klientów, ma kluczowe znaczenie dla skuteczności ochrony przed cyberzagrożeniami.

Wyzwania te są dostrzegane również na poziomie globalnym. Światowe Forum Ekonomiczne (*World Economic Forum* – WEF) zwraca uwagę na zagrożenia związane z cyberbezpieczeństwem, wynikające m.in. z konfliktów geopolitycznych, rosnącej aktywności cyberprzestępców oraz wdrażania nowych technologii, takich jak sztuczna inteligencja (SI). Czynniki te zwiększają podatność systemów informatycznych na ataki. W raporcie *Global Cybersecurity Outlook 2025* WEF podaje, że 60% przebadanych organizacji uważa, że napięcia geopolityczne wpłynęły na zmianę w ich postrzeganiu ryzyka. Jedna trzecia dyrektorów zarządzających (CEOs) obawia się działań o charakterze szpiegowskim, w tym utraty wrażliwych danych lub własności intelektualnej. Z kolei 45% dyrektorów zarządzających obawia się głównie zagrożeń dla ciągłości operacyjnej oraz zakłóceń przebiegu procesów biznesowych, w tym utrudnień w funkcjonowaniu kanałów dostaw. Według raportu WEF, 66% przebadanych organizacji uważa, że SI może negatywnie wpłynąć na cyberbezpieczeństwo. Jednocześnie tylko 37% respondentów posiada w swoich jednostkach procedury umożliwiające ocenę bezpieczeństwa wdrażanych rozwiązań opartych na sztucznej inteligencji, co powoduje dość paradoksalną sytuację: mimo wysokiej świadomości zagrożeń związanych z SI, wiele organizacji wdraża tego typu technologie w bardzo szybkim tempie, często pomijając niezbędne audyty bezpieczeństwa.

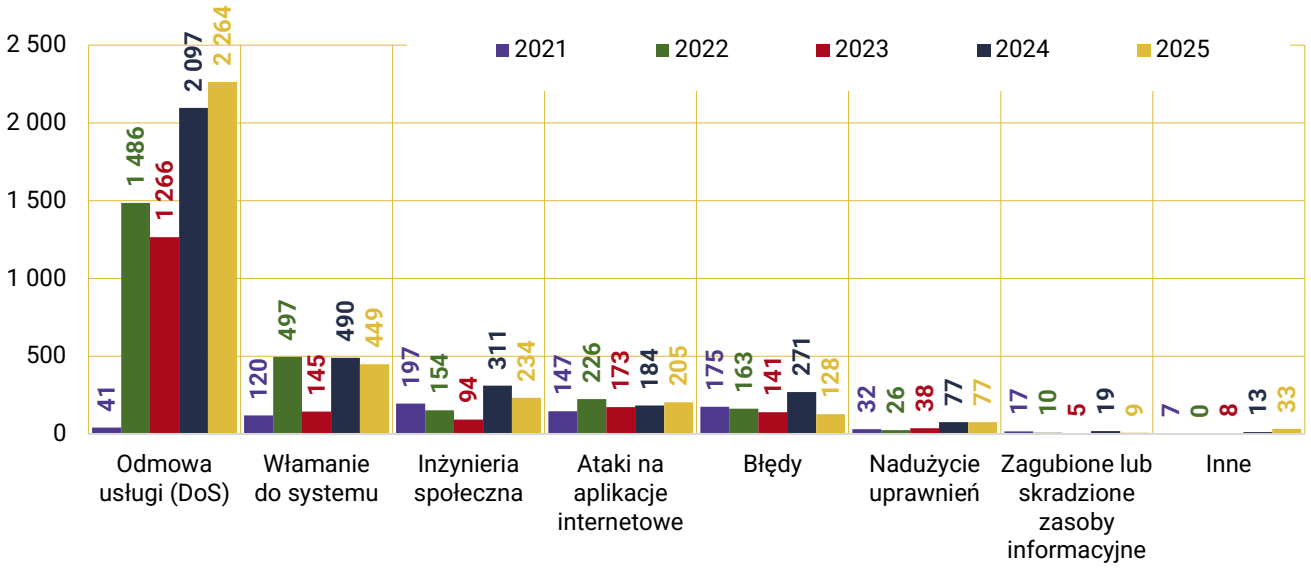
Aby dokładniej zobrazować skalę i charakter zagrożeń dla sektora finansowego, warto sięgnąć po konkretne dane obejmujące dłuższy okres, co pozwala uchwycić dynamikę zmian. Takie podejście umożliwia nie tylko identyfikację aktualnych zagrożeń, ale również ich zmiany w czasie. Wartościowym źródłem informacji w tym obszarze są coroczne raporty firmy Verizon – *Data Breach Investigations Report*. Przedstawiają one globalny obraz incydentów naruszenia cyberbezpieczeństwa – z podziałem na kategorie oraz sektory, w których wystąpiły. Verizon analizuje corocznie ponad 20 000 incydentów z różnych branż, co pozwala na identyfikację trendów i specyfiki zagrożeń w poszczególnych obszarach gospodarki (Verizon 2025).

Na potrzeby niniejszego raportu skoncentrowano się na liczbie i dynamice incydentów dotyczących globalnego sektora finansowego, zidentyfikowanych przez Verizon w ciągu ostatnich pięciu lat (Wykresy 5–6). Zgodnie z definicją przyjętą w raportach Verizon, incydentem określa się każde zdarzenie, które prowadzi do naruszenia poufności, integralności lub dostępności zasobów informacyjnych organizacji. Aby ułatwić analizę incydentów pod kątem ich podobieństwa, firma Verizon wprowadziła kategorie incydentów określane jako wzorce. Strukturę i dynamikę wzorców incydentów w sektorze finansowym na przestrzeni ostatnich pięciu lat zaprezentowano na Wykresie 5. Obecnie dominującym wzorcem w sektorze finansowym jest **odmowa usługi** (*Denial of Service* – DoS), wykazująca od 2020 roku wyraźny trend wzrostowy. Może to świadczyć o nasilają-

33 Oczywiście, rola banków będzie zależna od obowiązującego w danym kraju modelu systemu finansowego. Zdecydowanie większa jest ona w modelu uniwersalnym (europejskim), typowym także dla gospodarki polskiej.

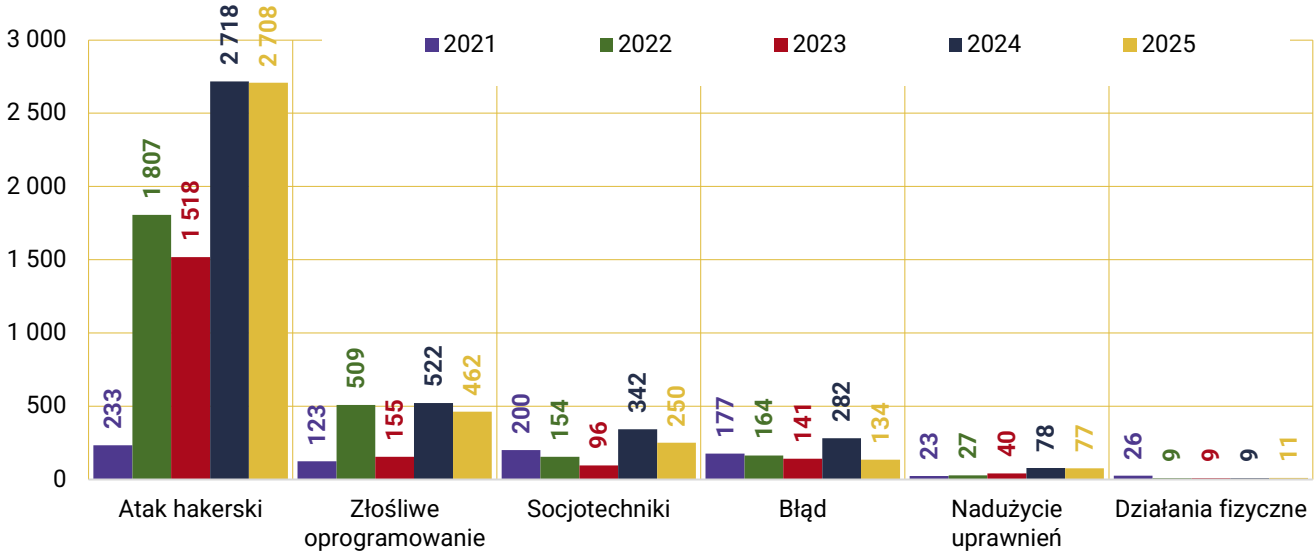
cych się próbach zakłócenia dostępności zasobów informacyjnych instytucji finansowych na całym świecie. Do często występujących w sektorze finansowym wzorców incydentów należą również: włamania do systemów, inżynieria społeczna, ataki na aplikacje internetowe oraz błędy – zarówno po stronie klientów, jak i pracowników, administratorów czy programistów.

Wykres 5. Wzorce incydentów cyberbezpieczeństwa w sektorze finansowym raportowane w latach 2021–2025



Źródło: Opracowanie własne na podstawie danych pochodzących z Verizon Data Breach Investigations Report z lat 2021–2025.

Wykres 6. Kategorie działań prowadzących do wystąpienia incydentu w sektorze finansowym, raportowane w latach 2021–2025



Źródło: Opracowanie własne na podstawie danych pochodzących z Verizon Data Breach Investigations Report z lat 2021–2025.

Oprócz analizy wzorców incydentów, istotne jest również zidentyfikowanie działań, które doprowadziły do ich wystąpienia, czyli bezpośrednich przyczyn. Strukturę i dynamikę przyczyn incydentów w sektorze finansowym na przestrzeni ostatnich pięciu lat przedstawiono na Wykresie 6. W sektorze tym dominującą, a jednocześnie dynamicznie rosnącą przyczyną incydentów cyberbezpieczeństwa są **ataki hakerskie**. Taki trend może wynikać z dwóch głównych czynników. Pierwszym z nich jest intensyfikacja globalnej rywalizacji geopolitycznej, która coraz częściej przybiera formę *proxy wars* prowadzonych w cyberprzestrzeni (Pinto 2024). Drugim czynnikiem jest przyspieszona transformacja cyfrowa, która została niejako wymuszona przez pandemię COVID-19, wiążąca się z szybkim wdrażaniem nowych rozwiązań technologicznych, co mogło, wskutek nadmiernego pośpiechu, prowadzić do uchybień w zakresie bez-

pieczeństwa systemów informatycznych (Conaway 2020). Innymi często występującymi przyczynami incydentów w sektorze finansowym były następujące działania: wykorzystanie złośliwego oprogramowania (ang. *malware*), ataki socjotechniczne oraz błędy ludzkie.

Poza incydentami bezpieczeństwa, raporty firmy Verizon koncentrują się również na analizie **wycieków danych**. Zgodnie z przyjętą definicją, wyciekiem danych jest incydent, którego skutkiem jest potwierdzone ujawnienie informacji nieupoważnionemu podmiotowi. W raporcie *Data Breach Investigations Report* z 2025 roku wskazano, że 35% wycieków dotyczyło danych wewnętrznych organizacji finansowych, 54% obejmowało dane osobowe użytkowników, a 22% dotyczyło danych uwierzytelniających. Aż 78% zagrożeń skutkujących wyciekiem danych pochodziło z zewnątrz organizacji, co stanowi znaczny wzrost w porównaniu z raportem z 2021 roku, kiedy odsetek ten wynosił 56%. Wśród motywacji sprawców dominowały korzyści finansowe, które odpowiadały za 78% wycieków. Natomiast działania o charakterze szpiegowskim stanowiły 12% przypadków. Choć udział działań szpiegowskich może wydawać się stosunkowo niewielki, to jednak niepokojąca jest jego dynamika: w 2023 r. motyw szpiegowski stanowił 3% wycieków, w 2024 r. 5%, a w 2025 r. już 12%.

Według publikacji Europejskiego Banku Centralnego, ataki cybernetyczne sponsorowane przez rządy obcych państw (ang. *state-sponsored cyberattacks*) stanowią jedno z głównych zagrożeń dla stabilności sektora finansowego – nie tylko bezpośrednio, jako ataki na poufność czy integralność danych, lecz także w sposób pośredni, poprzez destabilizację infrastruktury krytycznej państwa oraz życia obywateli (Wendelborn i in., 2025). Tego rodzaju ataki zazwyczaj nie są przeprowadzane bezpośrednio przez państwowe jednostki wojskowe lub wywiadowcze, lecz przez wyspecjalizowane, powiązane z państwem podmioty (ang. *state-nexus actors*) dysponujące zaawansowaną wiedzą informatyczną, które wraz z grupami cyberprzestępczymi klasyfikowane są jako tzw. grupy Zaawansowanego Trwałego Zagrożenia (ang. *Advanced Persistent Threat* – APT) (Cole 2013). Grupy APT charakteryzują się powtarzalnym i długotrwałym dążeniem do realizacji swoich celów, zdolnością adaptacji do mechanizmów obronnych atakowanego podmiotu oraz determinacją w utrzymywaniu intensywności ataku, aż do osiągnięcia zamierzonego rezultatu (NIST, 2011), dzięki zapewnieniu znacznych zasobów technicznych i finansowych pochodzących ze świata przestępczego lub finansowania przez rządy państw.

Przykładem grupy APT dokonującej cyberataków na sektor finansowy jest powiązana z Koreą Północną grupa Lazarus, znana również pod nazwą APT38. Do działań przypisywanych tej grupie należy m.in. kradzież kryptowalut i tokenów o wartości około 275 milionów dolarów z giełdy KuCoin w 2020 roku (Chainanalysis, 2020). Jednym z najbardziej zuchwałych i niepokojących ataków tej grupy była kradzież około 81 milionów dolarów z Banku Bangladeszu w 2016 roku. Atak ten był możliwy dzięki wykorzystaniu słabości w serwerach systemu obsługującego transakcje SWIFT. Grupę Lazarus charakteryzuje stosowanie złożonych i zróżnicowanych technik ataku, takich jak: wykorzystanie podatności typu *zero-day*[34], oszustwa typu *spear phishing*[35], dezinformacja, złośliwe oprogramowanie, *backdoory*[36] (furtki w oprogramowaniu), oraz *droppery*[37] (programy infekujące systemy) (Radware n.d.).

Innym przykładem grupy APT, która zasłynęła z ataków na sektor finansowy, jest powiązana z Rosją grupa Carbanak, znana również pod nazwą FIN7. Do działań przypisywanych tej grupie należy wytransferowanie aktywów o łącznej wartości około miliarda dolarów z około stu instytucji finansowych na całym świecie. Grupa Carbanak, wykorzystując fałszywe wiadomości e-mail kierowane do pracowników instytucji finansowych (ang. *phishing*), doprowadziła do zainstalowania furtki w oprogramowaniu (ang. *backdoor*) na ponad stu komputerach. Umożliwiło to cyberprzestępcom przejęcie kontroli nad systemami bankowości internetowej, e-płatności, stanami kont klientów oraz bankomatami. Dzięki uzyskanym uprawnieniom, przestępcy podwyższali salda kont klientów, a następnie transferowali nadwyżki na zagraniczne rachunki (Kaspersky 2015). W niektórych krajach grupa Carbanak wypłacała gotówkę z bankomatów bez fizycznej interakcji z nimi, a środki były odbierane przez podstawione osoby (Securelist, 2015).

34 Podatność sprzętu lub oprogramowania, wcześniej nieznana producentowi lub użytkownikom, która może zostać wykorzystana do przeprowadzenia cyberataku.

35 Ukierunkowana forma socjotechniki (ang. phishingu) wymierzona w konkretny podmiot, zwykle z użyciem spersonalizowanej wiadomości mającej skłonić ofiarę do działań umożliwiających cyberatak.

36 Nieudokumentowany sposób uzyskania dostępu do systemu komputerowego.

37 Złośliwe oprogramowanie, którego celem jest dostarczenie i zainstalowanie w systemie ofiary innego złośliwego oprogramowania.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w raporcie dotyczącym zagrożeń cyberbezpieczeństwa w sektorze finansowym zwraca uwagę, że obok podmiotów powiązanych z państwami oraz grup cyberprzestępczych, poważnym źródłem zagrożenia są również tzw. haktywiści. W przeciwieństwie do grup APT nie dysponują oni zaawansowanymi kompetencjami informatycznymi ani znacznymi zasobami technicznymi i finansowymi. Ich siłą jest jednak liczba wolontariuszy, którzy, z pobudek ideologicznych lub motywowani korzyściami finansowymi (np. wynagrodzeniem w kryptowalutach), współdzielą swoje zasoby, wspierając cyberataki, takie jak rozproszona odmowa usługi (DDoS) czy *ransomware*[38] (ENISA, 2024).

Przykładem zorganizowanej grupy haktywistów jest powiązana z Rosją NoName057, która od czasu inwazji Rosji na Ukrainę prowadzi ataki na sektor finansowy w Ukrainie oraz państwach członkowskich NATO (ENISA, 2024). Grupie tej przypisuje się m.in. atak na strony internetowe duńskiego banku centralnego oraz dwóch duńskich banków komercyjnych w styczniu 2023 roku (Reuters, 2023).

Pewien pogląd co do prawdopodobieństwa wystąpienia określonego typu cyberzagrożenia w europejskich instytucjach finansowych może dać analiza częstotliwości występowania poszczególnych kategorii ataków. Dane na ten temat udostępnia Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) we wspomnianym wcześniej raporcie. Zgodnie z nim, w okresie od stycznia 2023 do czerwca 2024 najczęściej występowały ataki typu rozproszona odmowa usługi (DDoS), które stanowiły 46% wszystkich incydentów. Drugim najczęściej występującym typem ataków były zagrożenia dla poufności, integralności i dostępności danych – 15% przypadków. Ataki wykorzystujące socjotechniki odnotowano w 13% przypadków, a *ransomware* stanowił 10% incydentów. Pozostałe przypadki obejmowały oszustwa komputerowe, ataki z wykorzystaniem złośliwego oprogramowania, włamania do systemów komputerowych, ataki na kanały dostaw oraz zagrożenia sieciowe (ENISA, 2024).

Należy pamiętać, że częstotliwość występowania ataków w danej kategorii nie przesądza o ich dotkliwości dla instytucji finansowej. Nawet rzadko występujący atak może mieć ogromny wpływ na funkcjonowanie takiej instytucji. Dobrym przykładem ilustrującym tę uwagę jest wcześniej omawiany atak grupy Carbanak, która, wykorzystując socjotechniki, dokonała włamania do systemów bankowych, powodując miliardowe straty. Europejski Bank Centralny za najbardziej zagrażające sektorowi bankowemu ataki uznaje te wymierzone w dostawców usług IT oraz ataki typu *ransomware*, które zagrażają dostępności danych i mogą poważnie zakłócić ciągłość działania procesów w sektorze bankowym. Natomiast relatywnie mniejszą wagę przywiązuje do ataków typu rozproszona odmowa usługi (DDoS) (ECB, 2024).

2.3. Konsekwencje dla rynku kryptowalut

Pomimo zróżnicowanego postrzegania kryptowalut – od bezkrytycznego entuzjazmu po zdecydowane odrzucenie – obrót nimi stanowi istotny element codziennych transakcji finansowych. Kapitalizacja wszystkich kryptowalut osiągnęła w marcu 2026 r. poziom ok. 2,4 bilionów dolarów [39].

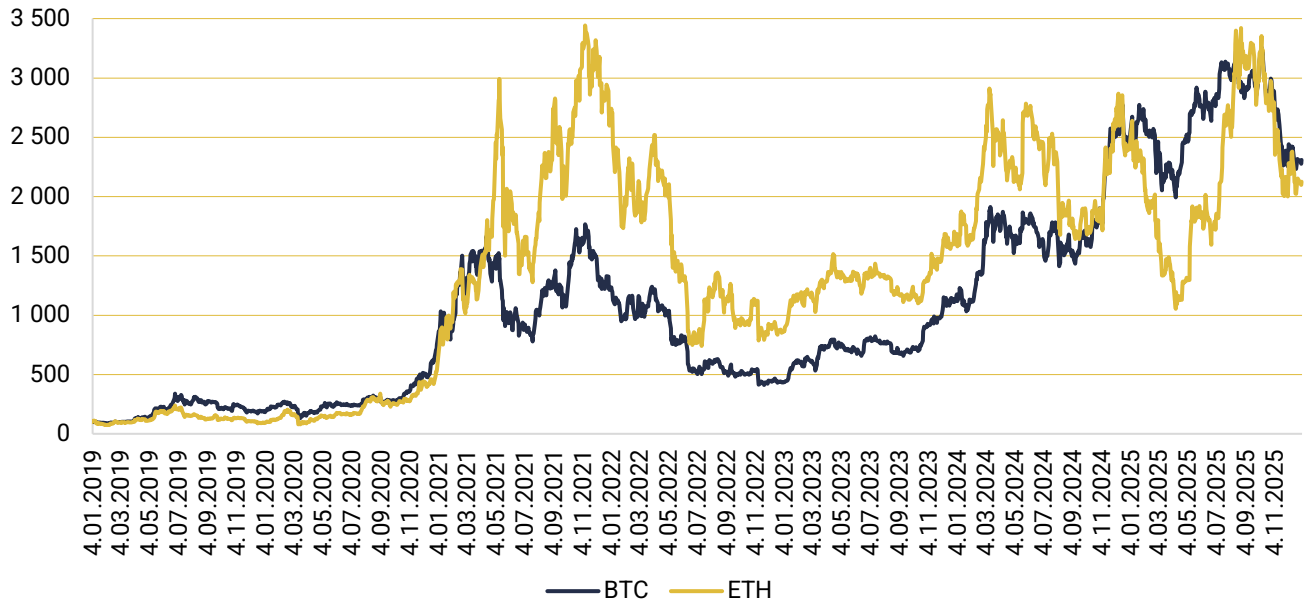
Intrygującym zjawiskiem w przypadku kryptowaluty Bitcoin jest tzw. „bardzo długo nieaktywna podaż" (ang. *ancient supply*), czyli liczba jednostek, które nie uczestniczyły w żadnych transakcjach przez ponad 10 lat. W czerwcu 2025 roku udział tej podaży wynosił około 17%, a jej kapitalizacja przekraczała 360 miliardów USD (Wainwright, 2025). Niezidentyfikowana część tej podaży może stanowić trwale utracone jednostki, które z przyczyn technicznych już nigdy nie powrócą do obrotu. Ze względu na trudności w ustaleniu podmiotów kontrolujących zasoby stanowiące „bardzo długo nieaktywną podaż", którymi mogą okazać się grupy powiązane z państwami (w tym grupy APT), istnieje ryzyko jej potencjalnego wykorzystania przez aktorów dążących do destabilizacji lub nawet załamania rynku kryptowalut oraz powiązanych z nimi instrumentów pochodnych – jako elementu wojny hybrydowej. Szacowanie liczby jednostek kryptowalut posiadanych przez poszczególne państwa opiera się głównie na fragmentarycznych danych publikowanych w serwisach internetowych. Według serwisu Bitcoin Treasuries, największymi państwowymi posiadaczami Bitcoina są Stany Zjednoczone i Chiny – każde z tych państw posiada niemal 200 000 jednostek, co stanowi ponad 30% dziennego wolumenu obrotu. Do innych znaczących posiadaczy należą Wielka Brytania (ponad 60 000 jednostek) oraz Ukraina (ponad 46 000 jednostek) (BiTBO, 2025).

38 *Ransomware* jest typem złośliwego (malware) oprogramowania, które blokuje dostęp do plików lub całego systemu, po czym szyfruje dane i żąda od zaatakowanego w ten sposób podmiotu okupu za przywrócenie dostępu.

39 W październiku 2025 r. wynosiła ona nawet ponad 4 biliony USD.

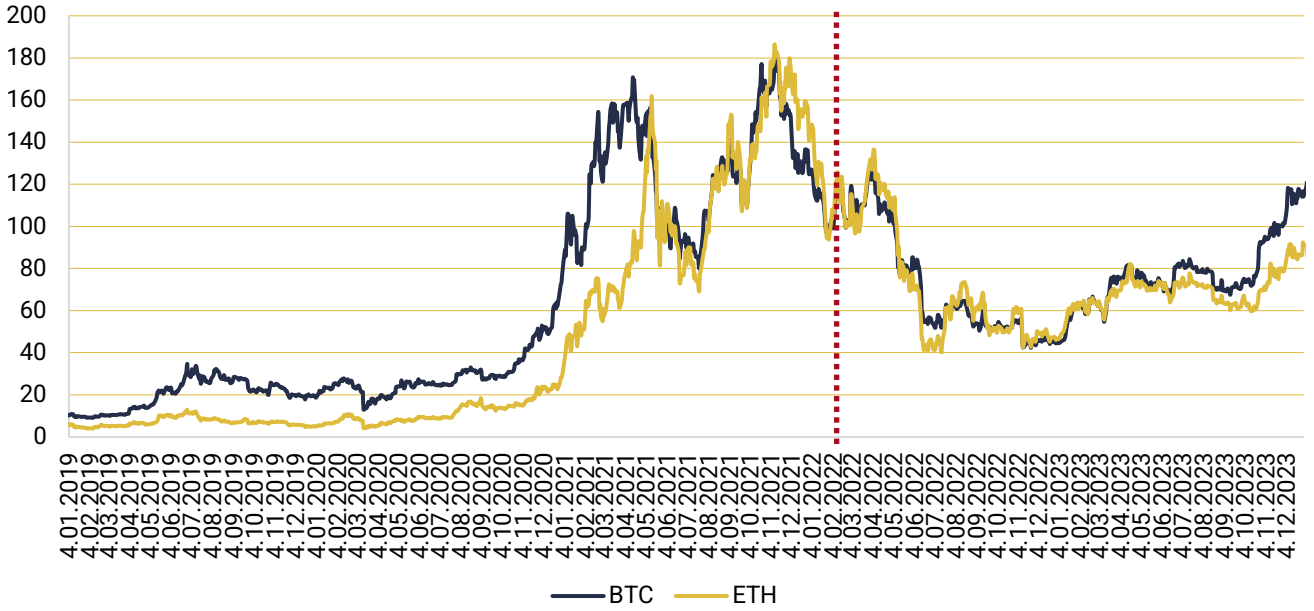
Historia rynku kryptowalut pokazuje jego podatność na silne wahania. Przykładowo, w okresie od września 2021 do maja 2022 roku wycena kryptowaluty Bitcoin (BTC) spadła z około 50 000 USD do około 31 000 USD[40]. W tym czasie spadek odnotowała kryptowaluta Ether (ETH) – z poziomu około 3 800 USD do około 1 900 USD. Zjawiska te uwidaczniają silny wpływ czynników makroekonomicznych, problemów wewnętrznych branży kryptowalut oraz napięć geopolitycznych na wycenę tych aktywów (Yahoo Finance 2025, 2025a). Jako ilustrację tych zjawisk można wskazać wykresy 7–8, obrazujące kształtowanie się indeksów kryptowalut w latach 2019–2025 w ujęciu ogólnym, oraz jako event study – gdzie podstawę indeksu wyznacza rozpoczęcie pełnoskalowej wojny na Ukrainie.

Wykres 7. Indeks kryptowalut – ujecie ogólne (02.01.2019=100)



Źródło: Opracowanie własne.

Wykres 8. Indeks kryptowalut – event study (24.02.2022=100)



Źródło: Opracowanie własne.

40 Wycena Bitcoina od początku roku do połowy lutego 2026 r. spadła o mniej więcej jedną czwartą, a od swojego szczytu – 126 272 USD 5 października 2025 r. – prawie o połowę.

Powszechnie uważa się, że kryptowaluty oparte na technologii łańcucha bloków są bezpieczne dzięki takim elementom ich architektury jak rozproszenie, algorytmy zapewniające spójność danych oraz zastosowanie zaawansowanej kryptografii. Jednak o bezpieczeństwie systemu informatycznego decyduje nie tylko jego architektura, lecz również szczegóły implementacyjne oraz niejawne założenia projektowe, które nie zostały uwzględnione w oficjalnej specyfikacji, a mogą stanowić źródło poważnych podatności.

W praktyce miało miejsce wiele udanych ataków na sieci blockchain, w których wykorzystano różnorodne podatności. Przykładem są ataki polegające na przejęciu ponad 50% mocy obliczeniowej sieci, co umożliwia manipulowanie zapisami w blokach. Ofiarami takich ataków padły m.in. Bitcoin Gold (Sharma, 2018) oraz Ethereum Classic (Voell, 2021). Sieć Ronin, wykorzystująca technologię blockchain do obsługi płatności w grze Axie Infinity, utraciła kryptowaluty o wartości ponad 600 milionów dolarów w wyniku ataku z użyciem furtki w oprogramowaniu (*backdoor*), która umożliwiła przejęcie kontroli nad węzłami odpowiedzialnymi za bezpieczeństwo transakcji (Warren-Kachelein, 2022). W 2016 roku doszło do głośnego ataku na inteligentny kontrakt[41] (*smart contract*) należący do organizacji „The DAO", działający w sieci Ethereum. Atakujący wykorzystali błędy w implementacji kontraktu i wytransferowali kryptowalutę Ether o wartości około 50 milionów dolarów (Mehar i in., 2017). Poza atakami zrealizowanymi w praktyce, w literaturze opisano również teoretyczne mechanizmy ataków. Przykładem są scenariusze ataków typu DDoS, skierowanych przeciwko węzłom sieci Ethereum (Li i in., 2021; Yaish i in., 2024). Powyższe przykłady stanowią jedynie fragment szerszego obrazu licznych ataków oraz zidentyfikowanych podatności związanych z systemami opartymi na technologii blockchain.

Z jednej strony operacje kryptowalutowe stanowią użyteczne narzędzie dla cyberprzestępców i grup APT, umożliwiając finansowanie działalności z pominięciem tradycyjnych systemów bankowych. Z drugiej strony, te same grupy stanowią realne zagrożenie dla funkcjonowania systemów kryptowalutowych, ponieważ mogą wykorzystać złożone, kaskadowe ataki z użyciem wielu metod — takich jak *phishing*, *droppery*, furtki w oprogramowaniu, sieci botnet, DDoS — w celu sparaliżowania działania systemu lub nawet istotnej manipulacji danymi transakcyjnymi zapisanymi w łańcuchu bloków.

2.4. Przepływy kapitałowe i bezpośrednie inwestycje zagraniczne

W ostatnich latach rosnące napięcia geopolityczne stały się jedną z kluczowych determinant międzynarodowych przepływów kapitału. W literaturze jednoznacznie wskazuje się, że wzrost ryzyka geopolitycznego prowadzi do istotnego ograniczenia napływu bezpośrednich inwestycji zagranicznych (BIZ, ang. *foreign direct investments* – FDI), przy czym skala i mechanizmy tego wpływu są zróżnicowane w zależności od poziomu rozwoju gospodarki, sektora oraz źródła i rodzaju ryzyka.

Ryzyko geopolityczne może oddziaływać na przepływy BIZ pomiędzy krajem goszczącym a krajem pochodzenia kapitału poprzez następujące czynniki: (1) tzw. dystans geopolityczny; (2) eskalację konfliktów; (3) sankcje; (4) restrykcje technologiczne oraz (5) wzrost niepewności regulacyjnej.

Dystans geopolityczny to, najogólniej, koncepcja określania odległości między państwami nie tylko w kilometrach, ale przede wszystkim poprzez sojusze, ideologię i bezpieczeństwo. Oparte na dużych próbach badania projektów *greenfield*[42] oraz transakcji fuzji i przejęć (*mergers and acquisitions* – M&A) pokazują, że tak rozumiany dystans (mierzony np. różnicami głosowań w ONZ) w coraz większym stopniu determinuje lokalizacje BIZ. Z analizy MFW dla lat 2003–2023 wynika, że znaczący wzrost dystansu geopolitycznego wiązał się ze spadkiem napływu BIZ o około 15%. Szczególnie widoczne było to po 2018 roku. Skala zjawiska najsilniejsza była w sektorach strategicznych, takich jak produkcja półprzewodników czy telekomunikacja (Aiyar i in., 2024). Podobne wnioski płyną z raportu *World Economic Outlook*, gdzie oszacowano podatność BIZ na zmiany względem dystansu geopolitycznego. Z uzyskanych rezultatów wynika, że wzrost „niezgodności" poli-

41 Inteligentny kontrakt jest działającym w sieci blockchain programem, który automatycznie wykonuje z góry określone reguły, a rezultat zapisuje w rejestrze blockchain.

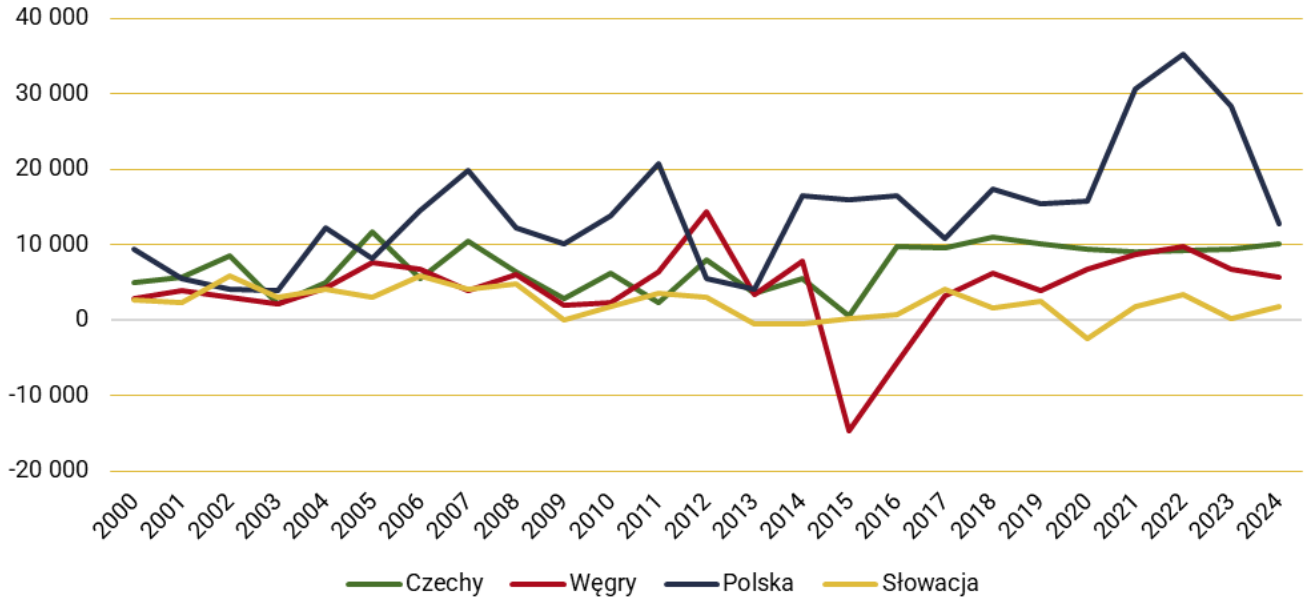
42 Mianem projektu *greenfield* ("zielone pole") określa się inwestycję lub przedsięwzięcie realizowane całkowicie od podstaw na niezabudowanym i nieuzbrojonym terenie. Obejmuje on budowę nowej infrastruktury, fabryk czy systemów IT bez konieczności adaptacji istniejących obiektów. Charakteryzuje się wysokimi kosztami początkowymi, ale daje pełną swobodę projektową

tycznej o jednostkę przyczynia się do obniżki napływu kapitału średnio o 12%. Konsekwencje dystansu geopolitycznego były przy tym szczególnie dotkliwe dla gospodarek wschodzących (Ahn i in., 2023).

Badania panelowe obejmujące kilkadziesiąt gospodarek wskazują przy tym, że wzrost indeksu GPR prowadzi do zjawiska określanego jako jednoczesna redukcja (ang. *retrenchment*) napływów i odpływów kapitału. W gospodarkach wschodzących obserwuje się wyraźny spadek BIZ, podczas gdy w krajach wysokorozwiniętych może wystąpić efekt ucieczki do „bezpiecznej przystani" (ang. *safe haven*), czyli relatywny wzrost napływu kapitału w okresach podwyższonego ryzyka[43] (Feng i in., 2023).

Raporty UNCTAD z ostatnich lat potwierdzają, że postępująca fragmentacja geopolityczna oraz wzrost barier inwestycyjnych (wprowadzane procedury przeglądu BIZ, kontrola eksportu, restrykcje itp.) niejako przeprofilowują mapę BIZ, prowadząc do regionalizacji i tzw. *friend-shoringu*, czyli lokowania produkcji i łańcuchów dostaw w krajach postrzeganych jako przyjazne, stabilne politycznie i militarnie, o zbliżonych systemach politycznych. W 2023 roku wartość BIZ wyniosła globalnie około 1,3 bln USD, pozostając na poziomie niższym niż we wcześniejszych latach, a finansowanie projektów infrastrukturalnych spadło o 26%, co w dużej mierze przypisywano właśnie napięciom geopolitycznym i niepewności regulacyjnej (UNCTAD, 2024). W 2024 roku odnotowano dalszy spadek BIZ o około 11% w porównaniu z 2024 rokiem; dodatkowo, napływ kapitałów koncentrował się coraz silniej w wąskiej grupie państw o zbliżonych systemach politycznych (UNCTAD, 2025).

Wykres 9. Napływ BIZ do wybranych krajów Europy Środkowej i Wschodniej w latach 2000–2025 (w mln USD, ceny bieżące)



Źródło: Opracowanie własne na podsatwie: Baza UNCTAD, https://unctadstat.unctad.org/datacentre/dataviewer/US.FdiFlowsStock, dostęp 9.5.2026.

Kształtowanie się BIZ w odniesieniu do Polski, Czech, Węgier i Słowacji przedstawiono na wykresie 9. Zwraca uwagę szczególnie kolaps BIZ w odniesieniu do Polski począwszy od 2023 r. Jak wynika z raportu PIE spadek inwestycji typu *greenfield* może wynikać ze spowolnienia w gospodarkach europejskich (zwłaszcza niemieckiej), ale i napięć geopolitycznych oraz niepewności biznesowej (Kopiński 2025).

Ograniczenie napływu BIZ w wyniku wzrostu ryzyka geopolitycznego wywołuje istotne skutki dla stabilności i funkcjonowania sektora bankowego. Przede wszystkim, spadek BIZ zmniejsza dostępność długoterminowego kapitału, co ogranicza finansowanie projektów inwestycyjnych i pogarsza perspektywy wzrostu gospodarczego; a tym samym spada jakość portfela kredytowego banków. Badania wskazują, że w warunkach nasilonej fragmentacji geopolitycznej i finansowej obserwuje się spadek rezerw walutowych, redukcję aktywów zagranicznych oraz wzrost kosztów finansowania, co zwiększa presję na płynność i kapitał regulacyjny instytucji finansowych (Alsadan i in., 2025). W krótkim okresie rośnie udział kredytów zagrożonych i koszty operacyjne, natomiast w długim okresie ograniczona dywersyfikacja ryzyka transgranicznego obniża odporność

43 W ujęciu sektorowym szczególnie wrażliwe są branże energetyczne i technologiczne (Lu i Liu, 2024).

banków na lokalne szoki. W rezultacie sektor bankowy, szczególnie w krajach zaliczanych do grupy *emerging markets*, staje się bardziej podatny na kryzysy płynnościowe i wymaga utrzymywania wyższych buforów kapitałowych. To z kolei dodatkowo jeszcze zmniejsza zdolność do wspierania inwestycji i wzrostu gospodarczego.

Reasumując, rosnące ryzyko geopolityczne ogranicza napływ kapitału zagranicznego poprzez trzy główne kanały:

- selektywność lokalizacji inwestycji i preferencję dla krajów „sojuszniczych";
- wzrost kosztów transakcyjnych i regulacyjnych związanych z kontrolą inwestycji;
- efekt niepewności, który opóźnia realizację projektów i zmniejsza skłonność do inwestycji, szczególnie w gospodarkach wschodzących.

Dodatkowo, wpływ GPR na sektor bankowy pogłębia ryzyko finansowe i ogranicza zdolność do absorpcji szoków, co w połączeniu z mniejszym napływem BIZ może prowadzić do trwałego obniżenia potencjału wzrostu w krajach najbardziej narażonych na geopolityczne napięcia.

2.5. Funkcjonowanie sfery gotówkowej i ryzyko odpływu depozytów

W kontekście ryzyka geopolitycznego szczególną uwagę należy zwrócić na – niestety dość często bagatelizowaną w kontekście dynamicznego rozwoju bankowości cyfrowej, proliferacji bezgotówkowych form płatności, kryptowalut czy walut cyfrowych banków centralnych (CBDC)[44] – kwestię dostępu i prawidłowego obiegu pieniądza gotówkowego. Tymczasem, odpowiednie kształtowanie zaopatrzenia w gotówkę w dobie rosnącego ryzyka geopolitycznego wydaje się być jednym z kluczowych warunków minimalizowania tego ryzyka oraz negatywnych konsekwencji.

Wynika to z wielu elementów. **Po pierwsze**, gotówka stanowi swoisty bufor bezpieczeństwa dla społeczeństwa, co wiąże się z tzw. motywem przezornościowym utrzymywania pieniądza (zob. Keynes, 1985). W tym właśnie kontekście można interpretować występujący w ostatnich latach tzw. **paradoks gotówki** (zob. np. Jiang i Shao, 2020): mimo wzrostu wolumenu rozliczeń bezgotówkowych, udział gotówki w obiegu pieniężnym bynajmniej nie maleje – jest ona bowiem utrzymywana przez społeczeństwo nie do celów transakcyjnych, ale jako rezerwa, nawet mimo tego, iż nie wiążą się z nim odsetki[45]. **Po drugie**, gotówka zapewnia **niezależność od infrastruktury cyfrowej** – pozostaje funkcjonalna nawet w przypadku ataków cybernetycznych na systemy płatnicze lub infrastrukturę bankową. To szczególnie istotne dla flankowego kraju NATO, jakim jest Polska, zwłaszcza w kontekście opisywanego nasilenia cyberataków na polskie instytucje w ostatnich miesiącach. **Po trzecie**, gotówka jest bezpośrednim zobowiązaniem krajowego banku centralnego, co wzmacnia suwerenność państwa w polityce pieniężnej. Jak opisywano to w części 2, w czasach napięć geopolitycznych waluta stanowi kluczowy element niezależności ekonomicznej i instrument rywalizacji geopolitycznej. **Po czwarte**, gotówka jest odporna na zakłócenia energetyczne. Nie wymaga ona elektryczności ani łączności internetowej, co czyni ją niezastąpioną w sytuacjach kryzysowych, np. coraz częstszych *blackoutów*, ale i w obliczu potencjalnych ataków na infrastrukturę energetyczną. **Po piąte** wreszcie, gotówka może chronić przed sankcjami finansowymi. W kontekście opisywanej weaponizacji sfery monetarnej, stanowi ona alternatywny kanał rozliczeń, który trudniej jest zablokować z zewnątrz.

Reasumując, w kontekście ryzyka geopolitycznego gotówka pełni rolę **ostatecznego, niezależnego instrumentu płatniczego**, który funkcjonuje niezależnie od infrastruktury cyfrowej. W sytuacjach kryzysowych (konfliktu zbrojnego, cyberataków, załamania infrastruktury energetycznej, upadku centrów decyzyjnych) gotówka pozostaje środkiem wymiany i swoistą „polisą ubezpieczeniową", gdy systemy elektroniczne zawodzą. Dość zatem nieoczekiwanie forsowanie walut cyfrowych czy wyłącznie bezgotówkowych rozliczeń może – nieoczekiwanie – osłabiać odporność na ryzyka geopolityczne.

Zdolność danego kraju do zapewnienia odpowiedniego zaopatrzenia w gotówkę w warunkach kryzysu geopolitycznego można zatem traktować jako istotny wymiar i swoisty probierz suwerenności monetarnej[46]. Ważny jest tutaj również wymiar spo-

44 Formułowano nawet poglądy o nieuchronności przejścia do tzw. *cashless economy* (zob. np. Marszałek i Szarzec, 2022). Poglądy te straciły jednak w ostatnich latach na znaczeniu, między innymi właśnie wskutek nasilenia ryzyka geopolitycznego.

45 Zjawisko to widoczne jest również w Polsce.

46 Dotyczy to nawet wymiaru technicznego – jeśli kraj jest uzależniony od importu specjalistycznego papieru, farb drukarskich czy technologii produkcji banknotów, jego autonomia jest ograniczona.

łeczny: w krajach o wysokim ryzyku geopolitycznym (np. sąsiadujących z konfliktami) ludzie trzymają więcej gotówki jako formę samoobrony przed niepewnością; samo w sobie może to być wskaźnikiem postrzegania ryzyka i bezpieczeństwa przez obywateli.

Pojawia się tu dość paradoksalna sytuacja: im bardziej społeczeństwo jest „ucyfrowione", a nowe technologie są szeroko stosowane w sferze finansowej, tym większe może być zapotrzebowanie na gotówkę w sytuacji kryzysu (brak bowiem alternatyw analogowych). Wtedy jednak może wystąpić kolejny problem – im mniej ludzi (szczególnie wśród młodszego pokolenia) i instytucji jest przyzwyczajonych do posługiwania się gotówką, tym większy chaos w przypadku konieczności powrotu do niej.

Z kwestią utrzymywania gotówki wiąże się inne zagadnienie, istotne z punktu widzenia ryzyka geopolitycznego, czyli kwestia potencjalnego odpływu depozytów. Bardziej szczegółowo zagadnienia te zostaną zaprezentowane w kolejnej części opracowania, dotyczącej już konkretnych mechanizmów i kanałów wpływu ryzyka geopolitycznego na banki. Tutaj wypada wskazać, iż wzrost ryzyka geopolitycznego oraz jego manifestacje (np. cyberatak, działania dezinformujące obcych wywiadów czy nawet atak kinetyczny) mogą w oczywisty sposób wywołać niepokój lub nawet panikę wśród klientów banków, prowadzącą do masowego wycofywania wkładów utrzymywanych przez nich w bankach. Ogranicza to płynność tych instytucji, utrudnia proces zarządzania aktywami i pasywami, a w perspektywie może nawet prowadzić do systemowego kryzysu bankowego. Ryzyko geopolityczne i jego postrzeganie wiążą się tu ściśle z kwestiami zaufania do instytucji bankowych, nadzorczych i całego aparatu państwowego, w tym zwłaszcza do mechanizmów stabilizujących gospodarkę w ogóle, a system finansowy w szczególności. Najnowszymi przykładami takich sytuacji są pandemia COVID-19 oraz rosyjska agresja na Ukrainę.

Warto tu zwrócić uwagę zwłaszcza na to ostatnie zdarzenie. Bezpośrednio przed rozpoczęciem przez Federację Rosyjską pełnoskalowej agresji w lutym 2022 r., Narodowy Bank Ukrainy (NBU) identyfikował ryzyko masowego wycofywania depozytów w przypadku eskalacji konfliktu zbrojnego, co umożliwiło szybkie uruchomienie wcześniej przygotowanych instrumentów stabilizacyjnych. NBU wdrożył pakiet nadzwyczajnych działań mających na celu ograniczenie ryzyka odpływu depozytów oraz utrzymanie stabilności sektora bankowego. Priorytetem władz monetarnych była stabilizacja rynku walutowego i przeciwdziałanie gwałtownej, niekontrolowanej dewaluacji hrywny, która mogłaby dodatkowo nasilić presję na wypłaty środków z banków (National Bank of Ukraine, 2022).

W tym celu NBU czasowo wprowadził administracyjnie ustalony tymczasowy kurs hrywny, prowadził interwencje na rynku walutowym oraz nałożył restrykcje na przepływy kapitałowe, w tym ograniczenia dotyczące transferów zagranicznych w walutach obcych oraz wypłat środków z rachunków walutowych. Po rozpoczęciu działań wojennych wprowadzono również dzienne limity wypłat gotówki w hrywnach, ustalone na poziomie 100 000 UAH na osobę. Rozwiązanie to miało na celu zapewnienie dostępności gotówki w bankomatach, równomierne rozłożenie wypłat w czasie oraz ograniczenie impulsywnych reakcji deponentów w warunkach podwyższonej niepewności. Równolegle NBU dążył do utrzymania ciągłości funkcjonowania sektora bankowego, w szczególności kanałów zdalnych. W tym celu bank centralny dopuścił możliwość migracji systemów informatycznych banków do infrastruktury chmurowej zlokalizowanej poza granicami kraju, m.in. w państwach Unii Europejskiej, Stanach Zjednoczonych i Kanadzie.

Jednocześnie NBU aktywnie promował obrót bezgotówkowy, nie wprowadzając ograniczeń dla płatności bezgotówkowych w hrywnach. Integracja ukraińskiego sektora bankowego z międzynarodowym systemem finansowym umożliwiła obywatelom, którzy opuścili kraj w wyniku wojny, dostęp do środków zgromadzonych na rachunkach bankowych za granicą oraz realizację płatności kartowych. Istotnym elementem działań stabilizacyjnych była również szybka, spójna i oparta na danych komunikacja NBU, która przyczyniła się do utrzymania zaufania społecznego i ograniczenia ryzyka wystąpienia runu na banki. W rezultacie, po początkowym, relatywnie niewielkim spadku poziomu depozytów w marcu 2022 r., zarówno depozyty gospodarstw domowych, jak i przedsiębiorstw szybko się odbudowały, a następnie wykazywały tendencję wzrostową, potwierdzając skuteczność zastosowanych instrumentów stabilizacyjnych (Drobiazko, 2024).

Wnioski z doświadczeń ukraińskich wskazują zatem, że ryzyko odpływu depozytów w warunkach podwyższonej niepewności geopolitycznej ma charakter silnie behawioralny i zależy w dużej mierze od zaufania do instytucji finansowych oraz wiarygodności polityki państwa. Ponadto kluczowe znaczenie ma tu wcześniejsze wypracowanie określonych rozwiązań oraz scenariuszy potencjalnych działań.

Część 3. Ryzyko geopolityczne w działalności banków – mechanizmy, konsekwencje, sposoby ograniczania

3.1. Kanały odziaływania ryzyka geopolitycznego na banki

W kontekście dotychczasowych rozważań oczywiste jest, że realizacja (materializacja) poszczególnych rodzajów ryzyka geopolitycznego musi mieć poważne następstwa dla stabilności systemu finansowego. Niewątpliwie ryzyko geopolityczne i jego manifestacje będą negatywnie wpływać na stabilność systemu finansowego. Wpływ ten jest złożony, daleki od mechanicznych, automatycznych relacji i odbywa się rozmaitymi kanałami, odnoszącymi się zarówno do nominalnej, jak i realnej sfery gospodarki; cechuje się też zróżnicowanym rozkładem czasowym

Na dość ogólnym poziomie, można wyróżnić cztery główne kanały przenoszenia szoków geopolitycznych na system finansowy (por. BIS, 2024; Cheng i Chiu, 2018; ECB, 2024; E&Y, 2025; NBP, 2024):

1. **Kanał gospodarki realnej** – zmniejszenie produkcji na skutek zakłóceń w funkcjonowaniu łańcuchów dostaw i transakcji handlowych, skutkujące niedostępnością środków produkcji (w tym surowców) lub wzrostem ich cen. Rezultatem finalnym może być wolniejsze tempo wzrostu gospodarczego – także wskutek gorszych nastrojów konsumentów i producentów oraz trudniejszych warunków finansowania, zwłaszcza w krajach z wysokim lub rosnącym długiem publicznym. Niski wzrost gospodarczy lub recesja i/lub podwyższona inflacja będą negatywnie oddziaływać na kondycję gospodarstw domowych i przedsiębiorstw, a w konsekwencji pogarszać ich zdolność do obsługi zadłużenia i zwiększać ryzyko kredytowe. Dodatkowo, niższy poziom aktywności gospodarczej i niekorzystne tendencje w zakresie stóp procentowych mogą także pogarszać sytuację w zakresie cen i płynności aktywów na rynkach finansowych. Im dłużej będzie trwać niekorzystna sytuacja w gospodarce realnej, tym większa liczba podmiotów będzie borykać się z obsługą zobowiązań wobec banków i w tym gorszej sytuacji znajdą się podmioty sektora.

2. **Kanał powiązań finansowych** – zaburzenia strumieni finansowych w postaci kredytów i pożyczek (w tym w ramach grup kapitałowych przedsiębiorstw niefinansowych), bezpośrednich inwestycji zagranicznych lub inwestycji portfelowych. W konsekwencji wystąpić mogą spadki wycen aktywów i nasilona zmienność stóp procentowych i kursów walutowych. Pogorszyć może się również wycena skarbowych papierów wartościowych utrzymywanych przez instytucje finansowe w portfelu handlowym, w szczególności w przypadku problemów z równowagą finansów publicznych (trudną do zapewnienia w warunkach konfliktów militarnych i konieczności sfinansowania zbrojeń).

3. **Kanał podwyższonej niepewności** – występują tu dwa rodzaje zależności: w odniesieniu do opisanych niekorzystnych tendencji w sferze realnej oraz tych ze sfery finansowej. W tym pierwszym przypadku zaburzenia w gospodarce realnej powodują spadek nastrojów i zaufania gospodarstw domowych oraz przedsiębiorstw, co w konsekwencji prowadzi do zmniejszenia wydatków konsumpcyjnych i inwestycyjnych. Dodatkowo osłabia to dynamikę wzrostu gospodarczego i zwiększa ryzyko kredytowe banków. W drugim natomiast przypadku niepewność dotycząca kategorii nominalnych, finansowych skutkuje wyższą zmiennością cen i wyższą awersją do ryzyka na rynkach finansowych. To zaś zwiększa koszt kredytu (czy szerzej, finansowania procesów gospodarczych) lub powoduje ograniczenie dostępności kredytu w wyniku trudności z oszacowaniem ryzyka kredytowego potencjalnych kredytobiorców lub odpływem kapitału w kierunku bezpiecznych inwestycji (ang. *safe havens*).

4. **Kanał ryzyka operacyjnego** – konsekwencje skutecznych cyberataków (zob. sekcja 2.2) na infrastrukturę krytyczną danego kraju, instytucje finansowe i ich systemy informatyczne lub dostawców ich kluczowych systemów informatycznych.

Możliwe jest także inne, bardziej szczegółowe ujęcie kanałów, za pośrednictwem których ryzyko geopolityczne wpływa na funkcjonowanie systemu bankowego. Przedstawiono je na Rysunku 3., dekomponując niejako cztery wskazane powyżej ogólne kanały. Zaprezentowany tam sposób klasyfikacji kanałów oddziaływania ryzyka geopolitycznego na banki w bezpośredni sposób wskazuje na poszczególne obszary działania tych instytucji. Stanowi także

dobry punkt wyjścia do rozważenia konsekwencji, jakie realizacja tego ryzyka ma dla systemu bankowego, jak i jego poszczególnych elementów (zob. punkt 3.2.).

Rysunek 3. Kanały oddziaływania ryzyka geopolitycznego na system bankowy

Źródło: Opracowanie własne.

Kanał cyberbezpieczeństwa obejmuje wszelkie kwestie dotyczące zagrożenia dla bankowych systemów informatycznych (w tym te scharakteryzowane w punkcie 2.2). W szczególności można tu wskazać na: ataki DDoS na infrastrukturę bankową, *ransomware* paraliżujące systemy transakcyjne, ataki na system SWIFT i rozliczenia międzybankowe, sabotaż systemów *back office* i bankowych baz danych czy wreszcie dezinformacje podważające zaufanie do konkretnych instytucji. Banki padają tu bezpośrednią ofiarą tego typu działań.

Kanał **infrastruktury krytycznej** ma charakter w dużym stopniu egzogeniczny względem systemu bankowego, dotyczący zagadnień ogólnokrajowych. Realizacja ryzyka geopolitycznego (np. wskutek ataku kinetycznego) dla banków może być częścią większych, nawet ogólnokrajowych zakłóceń, takich jak np. zakłócenia w dostawach energii elektrycznej (powodujące brak zasilania bankomatów, placówek, *data center*, instytucji okołobankowych, itp.) czy uszkodzenia infrastruktury telekomunikacyjnej. Kanał ten może jednak obejmować także manifestacje ryzyka odnoszone już konkretnie do banków: fizyczne zniszczenia infrastruktury bankowej (szczególnie w regionach przygranicznych) czy zakłócenia w łańcuchach dostaw (np. kart płatniczych, części zamiennych do bankomatów).

Kanał regulacji i sankcji również ma w pewnym stopniu charakter egzogeniczny. Odnosi się on bowiem, oprócz wpływu ryzyka geopolitycznego na wymogi kapitałowe (konieczność sprostania podwyższonemu ryzyku) i inne regulacje bankowe, także do problemów, jakie dla banków powodują sankcje międzynarodowe komplikujące transakcje z niektórymi kontrahentami czy inne ograniczenia w transakcjach międzynarodowych.

Kanałem częstej transmisji ryzyka geopolitycznego na banki są również kwestie **łańcuchów dostaw i powiązań** danego systemu bankowego z zagranicą. W szczególności, można tu wskazać takie obszary problemowe jak: uzależnienie od zagranicznych dostawców systemów IT (w skrajnych przypadkach, mogą oni nawet pochodzić z krajów potencjalnie wrogich); transmisja kryzysowych tendencji z zagranicznych banków-matek, zakłócenia w dostępie do usług outsourcingowanych czy wreszcie zależność od globalnej infrastruktury płatniczej (Visa, Mastercard, SWIFT).

Kanał kredytowy dotyczy konsekwencji, jakie ryzyko geopolityczne przynosi dla działalności kredytowej banków. W szczególności, może ono powodować pogorszenie jakości portfela kredytowego (wzrost *non-performing loans* – NPL) w wyniku spowolnienia gospodarczego, generującego problemy kredytobiorców korporacyjnych uzależnionych od handlu międzynarodowego, problemy kredytobiorców detalicznych w sytuacji wzrostu bezrobocia będącego następstwem gorszej koniunktury, a także problemy w obszarze kredytów hipotecznych przy spadku wartości zabezpieczeń. Dodatkowo, obsługa kredytów może ulec zakłóceniu lub wręcz wstrzymaniu wskutek niewypłacalności przedsiębiorstw w regionach dotkniętych konfliktem.

Kanał rynkowy odnosi się do ryzyka geopolitycznego jako czynnika zmieniającego warunki i parametry na rynkach finansowych. Można tu wskazać takie czynniki jak gwałtowne wahania kursów walutowych (złoty vs euro/dolar) uderzające w portfele walutowe, wzrost spreadów i zmienności na rynku obligacji, spadek wartości aktywów (akcji, kryptowalut, nieruchomości) w bilansach banków, a także wzrost kosztów refinansowania.

Oddziaływanie czynników geopolitycznych na **płynność** instytucji bankowych można postrzegać jako ten kanał, który „uruchamia się" jako jeden z pierwszych. Mianowicie materializacja ryzyka geopolitycznego (czy choćby sama jego większa percepcja) może wywołać takie zjawiska jak: masowe wypłaty gotówki przez klientów w reakcji na zagrożenia, run na banki wywołany paniką lub dezinformacją, zamrożenie dostępu do rynków międzybankowych, czy, szerzej, problemy z refinansowaniem ze źródeł zagranicznych, a także ucieczkę wkładów do „bezpieczniejszych" jurysdykcji czy w stronę aktywów trwałych.

W odniesieniu do **kanału operacyjnego** można wskazać takie zjawiska jak ograniczenia w czasie napięć geopolitycznych dostępności personelu (mobilizacja, ewakuacje), zakłócenia w funkcjonowaniu centrów operacyjnych, ograniczenie lub brak fizycznego dostępu do placówek bankowych w strefach zagrożonych czy, generalnie, problemy z ciągłością działania.

Jednym z bardziej wrażliwych obszarów jest **kanał zaufania i reputacji**. Jest on kluczowy dla stabilności systemów bankowych z uwagi na status banków jako instytucji zaufania publicznego, fakt, iż współczesne systemy bankowe działają na zasadzie cząstkowej rezerwy, czy wreszcie, na jeszcze bardziej ogólnym poziomie, fiducjarny charakter współczesnego pieniądza. W warunkach realizacji ryzyka geopolitycznego w którymś z jego wymiarów może nastąpić utrata zaufania klientów do poszczególnych banków czy nawet do systemu bankowego jako całości. Co szczególnie groźne, zaufanie może zostać podkopane wskutek kampanii dezinformacyjnej, opartej na całkowicie zmyślonych zarzutach i sprawach, skierowanej pod adresem konkretnej instytucji. W obecnej medialnej rzeczywistości nie stanowi to żadnego problemu, np. dla wywiadów obcych państw czy choćby agentów wpływu. Utrata zaufania może z kolei wywołać dalsze problemy poprzez efekt zarażania (ang. *contagion*), gdzie kolejne banki są „infekowane" negatywnymi tendencjami.

Kanał polityczny wiąże się z tym, że w obliczu ryzyka geopolitycznego system bankowy staje się niejako instrumentem realizacji ogólnej polityki państwowej, nakierowanej na utrzymanie konkurencyjności międzynarodowej, sprostanie wyzwaniom ze strony rywali geopolitycznych, czy, w skrajnym przypadku – uniknięcie starcia militarnego czy wojny hybrydowej. W takiej sytuacji może pojawić się ryzyko nacjonalizacji lub przymusowej restrukturyzacji, a banki mogą zostać zmuszone do współfinansowania wysiłku obronnego czy nasilonych zbrojeń. Może także wystąpić presja na (preferencyjne) kredytowanie sektorów strategicznych oraz motywowane względami politycznymi selektywne traktowanie banków ze względu na pochodzenie kapitału.

Ostatni kanał, **makroekonomiczny** ma charakter najbardziej ogólny. Ujmuje się tu wpływ, jaki ryzyko geopolityczne wywiera na banki poprzez ogólne agregaty, makroekonomiczne kategorie takie jak inflacja, tempo wzrostu gospodarczego czy *policy mix*.

Niezależnie od przebiegu zależności i mechanizmu transmisji ryzyka geopolitycznego poszczególnymi kanałami, trzeba jeszcze uwzględnić trzy kwestie. **Po pierwsze**, rozważane kanały nie działają w izolacji. Wprost przeciwnie, przeplatają się one, a ryzyko geopolityczne i jego manifestacje przebiegają często kilkoma kanałami równocześnie. Przykładowo, cyberatak lub manipulacja w mediach społecznościowych może zaburzyć zaufanie do danego banku, co może doprowadzić do wypłat przez zaniepokojonych klientów środków z tej instytucji, a w skrajnym wypadku – także do zjawiska całościowego runu na banki. Jeżeli w takiej sytuacji zawiedzie (lub zostanie celowo zaatakowana i uszkodzona lub wyeliminowana) infrastruktura energetyczna, to powstały kryzys może być trudny do opanowania, destabilizując system finansowy, a tym samym osłabiając całe państwo.

Po drugie, funkcjonowanie poszczególnych kanałów oraz przebieg zależności, który w nich zachodzi, nie są bynajmniej stałe, lecz wykazują się dużą zmiennością oraz różnym natężeniem[47]. Dodatkowo, system bankowy każdego kraju ma różne specyficzne dla siebie cechy i cechuje się różną wrażliwością na poszczególne aspekty ryzyka geopolitycznego, co sprawia, że pewne kanały są w nim szczególnie istotne i powinny być monitorowane szczególnie wnikliwie, inne zaś nie stanowią aż tak dużego problemu.

47 Można tu zauważyć analogię np. do kanałów transmisji polityki pieniężnej – przebieg zależności również jest w nich niepewny, daleki od automatyzmu, a końcowy efekt często jest nieoczekiwany i daleki od pożądanego. Tutaj, z uwagi na czynnik ryzyka wbudowany niejako implicite i będący de facto rdzeniem oraz katalizatorem całego łańcucha zależności, przebieg zdarzeń jest jeszcze bardziej skomplikowany i trudny do przewidzenia.

Po trzecie, wreszcie, nawet w obrębie jednego systemu bankowego, działanie poszczególnych kanałów, a tym samym wpływ ryzyka geopolitycznego na poszczególne banki, nie jest homogeniczne. Innymi słowy, różne instytucje będą mniej lub bardziej podatne na ryzyko geopolityczne. **Najbardziej narażone na nie wydają się być:**

1. Banki z wysoką ekspozycją międzynarodową:
   - banki z placówkami w regionach geopolitycznie niestabilnych;
   - banki finansujące handel zagraniczny z krajami objętymi napięciami/sankcjami;
   - banki z portfelami kredytowymi w walutach obcych, szczególnie z krajów „ryzykownych".
2. Banki o pewnej określonej strukturze własnościowej:
   - banki będące własnością zagranicznych inwestorów, zwłaszcza z krajów objętych sankcjami;
   - instytucje współpracujące z bankami państwowymi krajów autorytarnych;
   - banki z udziałowcami powiązanymi z reżimami politycznymi.
3. Banki specjalizujące się w określonych segmentach, w szczególności:
   - banki korporacyjne obsługujące międzynarodowe koncerny z wysoką ekspozycją na ryzyko geopolityczne;
   - banki finansujące projekty infrastrukturalne w niestabilnych regionach;
   - banki inwestycyjne aktywne na rynkach wschodzących.
4. Banki o specyficznym profilu działalności, wrażliwym z punktu widzenia zależności geopolitycznych:
   - banki silnie zaangażowane w finansowanie surowców energetycznych;
   - banki obsługujące klientów z branż obronnych;
   - banki obsługujące klientów branży technologicznej;
   - banki-korespondenci instytucji z krajów wysokiego ryzyka.
5. Banki o dużym, z różnych względów, znaczeniu dla krajowego systemu:
   - banki duże, ze złożoną strukturą operacji;
   - banki ważne systemowo, będące z tego powodu obiektem szczególnej uwagi potencjalnych rywali;
   - banki ważne ze względu na ich udział w aktywnościach i operacjach państwowych.

Próbując syntetycznie przedstawić narażenie i podatność poszczególnych banków na ryzyko geopolityczne, zestawiono Tabele 2–3. Przyjęto, iż banki są narażone na ryzyko geopolityczne w sposób bezpośredni i pośredni. Ten pierwszy dotyczy zwłaszcza instytucji z silnymi powiązaniami międzynarodowymi. Banki krajowe (dominacja kapitału krajowego) skoncentrowane na bankowości detalicznej, lokalnej, są zazwyczaj najmniej narażone, choć oczywiście nie całkowicie odporne na efekty pośrednie przez kanały makroekonomiczne. Charakterystykę bezpośredniego narażenia banków na ryzyko geopolityczne przedstawiono w Tabeli 2.

Tabela 2. Cechy banku oraz jego otoczenia jako czynnik bezpośredniego narażenia na ryzyko geopolityczne

Kreator (katalizator) ryzyka	Czynniki nasilające ryzyko geopolityczne	Konsekwencje ryzyka geopolitycznego
Właściciel/dominujący inwestor banku	• pochodzi z kraju, który jest zaangażowany w wojnę • pochodzi z kraju, który jest objęty sankcjami	• odsprzedaż udziałów i zmiana właściciela • negatywny wizerunek banku w kraju działalności
Region/kraj, w którym działa bank	• wojna w kraju/regionie • kraj sąsiaduje z krajem w stanie wojny • kraj jest objęty sankcjami politycznymi i gospodarczymi	• możliwe: likwidacja, przymusowa odsprzedaż spółek zależnych, nacjonalizacja banku • wyższa preferencja klientów do trzymania gotówki, wycofywanie z banków środków finansowych, run na banki

Źródło: *Opracowanie własne.*

Kreator (katalizator) ryzyka	Czynniki nasilające ryzyko geopolityczne	Konsekwencje ryzyka geopolitycznego
Bank centralny kraju, w którym działa bank	• w sytuacji kryzysu energetycznego, wzrostu cen energii i produktów (ang. *commodities*), zagrożenia wzrostu inflacji, podejmuje odpowiednie działania	• restrykcyjna polityka monetarna • dodatkowe wymagane środki bezpieczeństwa
Polityka fiskalna państwa, w którym działa bank	• w sytuacji wysokiego GPR, wysokich wydatków na zbrojenia nasilają się problemy budżetowe	• wzrost stawek podatkowych • wprowadzenie specjalnego podatku dla banków • wzrost zadłużenia rządów, wzrost oprocentowania papierów skarbowych, co wpływa na wzrost stopy procentowej

Źródło: *Opracowanie własne.*

Pośrednia ekspozycja na GRP związane jest natomiast z głównymi klientami tych banków – przedsiębiorstwami, które są zaangażowane na rynkach międzynarodowych lub w sektorach silnie zależnych od sytuacji za granicą (energetyczny, ropa, transport, logistyka). Zależności z tego wynikające ujęto w Tabeli 3.

Tabela 3. Czynniki pośredniego wpływu ryzyka geopolitycznego na banki, związane z ich głównymi klientami

Źródło ryzyka	Manifestacja ryzyka dla przedsiębiorstwa	Manifestacja ryzyka dla banku
• przedsiębiorstwo działa w krajach, które są w stanie wojny • przedsiębiorstwo działa w krajach, które są objęte sankcjami gospodarczymi i politycznymi	• utraty majątku, konfiskat, zniszczeń wojennych • ograniczenie handlu, rynków zbytu	• problemy ze spłatą zobowiązań przedsiębiorstwa (ryzyko kredytowe korporacyjne) • ograniczenie popytu na usługi bankowe • wyższe rezerwy na straty kredytowe
• nagłe wprowadzenie ceł i innych ograniczeń w handlu (wojny handlowe)	• wzrost cen dóbr i usług pośrednich • załamanie łańcuchów dostaw	• problemy ze spłatą zobowiązań przedsiębiorstwa (ryzyko kredytowe korporacyjne) • ograniczenie popytu na usługi bankowe • wyższe rezerwy na straty kredytowe
• działalność sektorach, w których istnieje zagrożenie blokadą morskich szlaków transportowych (ang. *choke points*) lub zamknięciem przestrzeni powietrznej	• wzrost kosztów (w tym kosztów energii)	• problemy ze spłatą zobowiązań przedsiębiorstwa (ryzyko kredytowe korporacyjne) • ograniczenie popytu na usługi bankowe • wyższe rezerwy na straty kredytowe
• ograniczenia w międzynarodowym handlu technologiami oraz kluczowymi surowcami (np. metale ziem rzadkich)	• wzrost kosztów • spadek konkurencyjności	• problemy ze spłatą zobowiązań przedsiębiorstwa (ryzyko kredytowe korporacyjne) • ograniczenie popytu na usługi bankowe • wyższe rezerwy na straty kredytowe
• fragmentaryzacja regulacyjna (wzrost liczby niespójnych regulacji i polityk podatkowych między państwami)	• wzrost kosztów	• problemy ze spłatą zobowiązań przedsiębiorstwa (ryzyko kredytowe korporacyjne) • ograniczenie popytu na usługi bankowe • wyższe rezerwy na straty kredytowe

Źródło: *Opracowanie własne.*

Jak wynika z Tabel 2–3 oraz wcześniejszych rozważań, poszczególne mechanizmy przenoszenia się ryzyka geopolitycznego wiążą się z określonymi obszarami działalności bankowej. Realizacja danego ryzyka geopolitycznego powoduje, poprzez mechanizm jego transmisji określonym kanałem, określone następstwa w funkcjonowaniu instytucji bankowej. Następstwa te nie są jednak, jak to wyjaśniono, identyczne dla poszczególnych rodzajów banków. Odmienna będzie też reakcja – nawet na taką samą manifestację ryzyka geopolitycznego – poszczególnych narodowych systemów bankowych. Niemniej, można wskazać na pewne powtarzające się wzorce i reakcje.

3.2. Konsekwencje ryzyka geopolitycznego dla systemów bankowych

Z rozważań wynika jednoznacznie, iż ryzyko geopolityczne stanowi poważne zakłócenie dla stabilności systemów bankowych. Negatywne zjawiska mogą przy tym, jak już częściowo przedstawiano w poprzednich sekcjach, dotyczyć rozmaitych aspektów funkcjonowania. Można je ujmować w rozmaitych przekrojach i klasyfikacjach. I tak, przykładowo, nawiązując do przedstawionych w poprzednich punktach kanałów oddziaływania/przenoszenia się ryzyka geopolitycznego, można jego konsekwencje dla instytucji bankowych ująć w sześć ogólnych grup, które ujęto na Rysunku 4.

Rysunek 4. Konsekwencje ryzyka geopolitycznego dla instytucji bankowych – ujęcie zagregowane

Źródło: Opracowanie własne.

Do konsekwencji dotyczących **działalności operacyjnej** można zaliczyć takie związane z ryzykiem geopolitycznym problemy jak: (1) zakłócenia w dostępie/użytkowaniu systemów płatniczych i infrastrukturze transgranicznej (szczególnie przy odcięciu od systemów typu SWIFT); (2) problemy z płynnością walutową i dostępem do finansowania w walutach rezerwowych; (3) skokowy wzrost kosztów zabezpieczeń cybernetycznych i ryzyka oraz konsekwencje ataków hybrydowych; (4) trudności z usługodawcami IT czy innymi kluczowymi dostawcami z regionów objętych konfliktami; (5) konieczność reorganizacji sieci placówek i operacji w strefach konfliktu lub sąsiadujących ze strefami konfliktu oraz (6) problemy z zapewnieniem kadry w obliczu eskalacji zagrożeń.

W odniesieniu do **ryzyka kredytowego i jakości portfela** konsekwencje są oczywiste: rośnie poziom tego ryzyka, a jakość portfela pogarsza się – rośnie wolumen „złych" kredytów. Dotyczy to zwłaszcza pogorszenia zdolności (ale i wiarygodności) kredytowej klientów korporacyjnych, szczególnie narażonych na konflikty. Wzrost NPL (*Non-Performing Loans*) następuje głównie w sektorach wrażliwych (handel międzynarodowy[48], łańcuchy dostaw, sektor energetyczny, wrażliwe technologie), ale wraz z przedłużaniem się sytuacji kryzysowych może on dotknąć również branż niepodatnych wprost na ryzyko geopolityczne. Pojawiają się także problemy z zabezpieczeniami kredytów (spadek wartości aktywów w strefach ryzyka), a z czasem – także niemożliwość odzyskania należności[49].

Zwiększa się także **ryzyko rynkowe**, z jakim konfrontowane są banki państwa, dotkniętego realizacją ryzyka geopolitycznego. Negatywne następstwa dla banków uwidaczniają się przy tym dość szybko, rzutując na podstawowe kategorie finansowe. Mianowicie, pojawiają się gwałtowne wahania kursów walutowych, wpływając na pozycje walutowe banków[50] jako reakcja na szoki geopolityczne, pojawiają się zmiany stóp procentowych, następuje przeszacowanie portfeli papierów wartościowych (szczególnie obligacji skarbowych), a także pojawiają się problemy z wyceną instrumentów pochodnych przy bardzo znaczącej ich zmienności.

Sytuację dodatkowo pogarsza wzrost **ryzyka płynności**, które w skrajnym przypadku może nawet przybrać formę runu na banki. Typowe i powszechne są też problemy z refinansowaniem na rynkach

48 Dotkliwie problem ten odczuły polskie firmy eksportujące do Rosji i Białorusi.

49 Banki mogą stracić dostęp do swoich aktywów w krajach objętych sankcjami lub konfliktami. Polskie banki doświadczyły tego z ekspozycjami na Rosję i Białoruś po 2022 r.

50 Nagłe i znaczne zmiany kursów walutowych krajów dotkniętych kryzysami geopolitycznymi mogą generować straty na pozycjach walutowych banków.

hurtowych, „zamrożenie" rynków międzybankowych i wspomniany ograniczony dostęp do walut obcych[51].

Ponadto, banki stają przed wyzwaniami związanymi z kwestiami **regulacji i *compliance***. W warunkach rosnącego ryzyka geopolitycznego zachodzi bowiem konieczność szybkiej (czasem wręcz niemal natychmiastowej) implementacji sankcji międzynarodowych. Zbyt późne ich wprowadzenie, czy też naruszenie sankcji może skutkować poważnymi konsekwencjami dla instytucji bankowej, która dopuściła się zaniedbań w tym obszarze. Tymczasem szybkie dostosowanie procedur generuje znaczące koszty i zwiększa ryzyko błędów. Innym problemem w tym zakresie może być konieczność dopasowania się do zwiększonych przez nadzorców wymogów kapitałowych, a także koszty związane z presją na *stress testing*, uwzględniający rozmaite niekorzystne scenariusze geopolityczne.

Czynnikiem, na który wpływają dotychczas charakteryzowane grupy konsekwencji ryzyka geopolitycznego, ale który ma także swoją własną specyfikę, jest **sytuacja klientów** bankowych. Są oni konfrontowani z rosnącą niepewnością, trudniejszym (lub po wyższym koszcie) dostępem do usług bankowych, w tym zwłaszcza tych związanych z aktywnością ponadnarodową.

Charakterystyczne jest, że skutki wzrostu ryzyka geopolitycznego i/lub jego manifestacji mają różny horyzont czasowy. Niektóre z nich pojawiają się natychmiast (kwestia dni/tygodni), jak na przykład załamanie kursów walutowych, spadki cen akcji czy problemy z płynnością na rynkach międzynarodowych. Wystąpienie innych może zająć miesiące, np. pogorszenie jakości portfeli bankowych wskutek wzrostu stopy NPL w ekspozycjach bezpośrednich, spadek rentowności z tytułu ograniczeń działalności czy koszty dostosowania się do nowych regulacji/sankcji. Inne z kolei negatywy ujawniają w horyzoncie 1–3 lat, przybierając formę trwałego wzrostu kosztów ryzyka, konieczności restrukturyzacji modeli biznesowych czy dokonania odpisów z tytułu utraconych aktywów. Wreszcie, ostatecznie pojawią skutki długofalowe (powyżej 3 lub nawet 5 lat), w postaci zmian geografii działalności danego banku, przekształcenia łańcuchów dostaw finansowych czy wreszcie nowych regulacji międzynarodowych.

Poszczególne negatywne następstwa ryzyka geopolitycznego dla systemu bankowego mogą być przy tym wzmacniane przez wzajemne powiązania i współzależności. Innymi słowy, może wystąpić mechanizm **tzw. kryzysu kaskadowego** (ang. *cascade disaster* – zob. np. Pescaroli i in., 2018) czy też **efektu kaskadowego**, rozpatrywanego na gruncie teorii systemów. Powiązania poszczególnych kanałów oddziaływania ryzyka geopolitycznego, obszarów, w jakich uwidaczniają się jego negatywne następstwa, tradycyjnych, bliskich związków między rynkami finansowymi, w połączeniu z kanałem zaufania i nastrojów, czy szerzej, ogromną rolą czynników psychologicznych, mogą przekształcić nawet stosunkowo niewielkie, lokalne napięcia w systemowy kryzys finansowy.

Zważywszy na fakt, że ryzyko geopolityczne powoduje zaostrzenie problemów w zasadzie w każdym z obszarów „tradycyjnych" rodzajów ryzyka bankowego, można zaryzykować tezę, iż stanowi ono swoiste „metaryzyko". Nie będąc odrębną kategorią w klasycznym podziale głównych ryzyk bankowych (kredytowych, rynkowych, operacyjnych, płynności), działa jako czynnik egzogeniczny, swoisty katalizator, który intensyfikuje wszystkie pozostałe kategorie ryzyka. Co więcej, materializacja ryzyka geopolitycznego prowadzi do skokowego wzrostu korelacji między różnymi typami ryzyka, słabo skorelowanymi w „normalnych" warunkach[52].

Kończąc rozważania nad konsekwencjami ryzyka geopolitycznego dla banków, należy wskazać, że niezależnie od już przedstawionych aspektów dotyczących poszczególnych płaszczyzn funkcjonowania instytucji bankowych, ryzyko to może wiązać się z zupełnie nowymi obowiązkami banków. Chodzi tu przede wszystkim o ich udział w potencjalnym finansowaniu wydatków zbrojeniowych, pośredniczenie w przekazywaniu funduszy na ten cel do odpowiednich sektorów gospodarki. Kwestie te będą poruszane w dalszej części opracowania.

51 Przykładowo, w okresach napięć dotyczących określonych lokacji, spready na obligacjach operujących tam banków rosną, co podnosi koszty pozyskiwania kapitału na rynkach międzynarodowych.

52 Niemniej, należy pamiętać, że ryzyko geopolityczne ma również własne, bezpośrednie kanały wpływu (np. sankcje, cyberataki). Nie zawsze prowadzi także do wzrostu wszystkich rodzajów ryzyka równocześnie, a jego wpływ jest zróżnicowany w zależności od kontekstu geograficznego i ekspozycji danej instytucji.

3.3. Sposoby ograniczania ryzyka geopolitycznego w systemach bankowych

3.3.1. Uwagi ogólne

Ryzyko geopolityczne można ograniczać na wiele sposobów, skupiając uwagę na rozmaitych płaszczyznach. W szczególności, można tu wskazać następujące obszary działań:

1. aspekty ponadnarodowe (organizacje i porozumienia międzynarodowe);
2. aspekty makroekonomiczne (polityka makroekonomiczna, polityka energetyczna, itp.);
3. aspekty regulacyjne i nadzorcze;
4. aspekty sektorowe, związane z działalnością operacyjną samych banków;
5. aspekty technologiczne (cyberbezpieczeństwo, zabezpieczenia, systemy rozproszone, itp.).

Przed prezentacją działań i mechanizmów w poszczególnych obszarach należy jeszcze raz podkreślić, że **ryzyko geopolityczne zasadniczo jest dla banków egzogeniczne**. Stąd, możliwości ich działania są tu z natury rzeczy ograniczone, a większa jest rola rządu, banku centralnego, podmiotów nadzorczych czy regulatorów. Ponadto, banki napotykają tu na pewne dylematy, jak choćby swoisty ***trade-off* stabilności z rentownością** – nadmierna ostrożność może obniżać zyski[53]. Bardzo trudne jest też przewidzenie pewnych zdarzeń, z którymi wiąże się nasilenie ryzyka geopolitycznego. Wreszcie, bardzo wysokie mogą okazać się koszty zabezpieczeń, a niektórych manifestacji ryzyka geopolitycznego w zasadzie nie sposób hedge'ować.

W dalszej części opracowania autorzy skoncentrują się na aspektach 3–5. Zagadnienia ponadnarodowe (aspekt 1) oraz makroekonomiczne (aspekt 2) wykraczają znacząco poza zakres rozprawy. Te pierwsze w ogóle wykraczają poza ramy ekonomii, pozostając w domenie polityki zagranicznej, stosunków międzynarodowych oraz współpracy międzynarodowej. Natomiast projektowanie oraz realizacja polityki makroekonomicznej, jak i poszczególnych polityk sektorowych (w tym zwłaszcza odpornej na ryzyka geopolityczne polityki energetycznej) są zagadnieniami tak szerokimi, że trudno pokusić się choćby o skrótowe ich przedstawienie, a przy tym w wielu aspektach wymagają już bardzo specjalistycznej wiedzy. Stąd, nie będą one stanowiły przedmiotu rozważań w niniejszym opracowaniu. Należy tylko zasygnalizować, że prawne, polityczne oraz makroekonomiczne aspekty ograniczania ryzyka geopolitycznego są swoistymi ramami, w których można (i powinno się) planować inne działania. Niewątpliwie, chcąc ograniczyć zagrożenia wynikające z ryzyka geopolitycznego powinno się zapewnić ścisłą koordynację tych ram – zarówno wzajemną, jak i z poszczególnymi działaniami podejmowanymi przez regulatorów oraz same instytucje bankowe. Warto także podkreślić, oprócz konieczności zaangażowania innych decydentów, rolę Narodowego Banku Polskiego, zarówno jako podmiotu polityki pieniężnej, instytucji nadzoru makroostrożnościowego i podmiotu odpowiedzialnego za administrowanie rezerwami walutowymi, niezmiernie ważnymi z punktu widzenia stabilności systemowej i bezpieczeństwa geopolitycznego.

3.3.2. Wybrane aspekty regulacyjne i nadzorcze

Ze względu na potencjalnie poważne konsekwencje, zagrożenia związane z cyberbezpieczeństwem podmiotów sektora finansowego mają kluczowe znaczenie. Problem ten od wielu lat znajduje się w centrum uwagi instytucji Unii Europejskiej oraz europejskich organów regulacyjnych. W celu zwiększenia bezpieczeństwa usług elektronicznych w sektorze finansowym opracowano szereg standardów i rekomendacji, takich jak SEPA Cards Framework oraz wytyczne dotyczące oceny bezpieczeństwa płatności internetowych, wydane przez Europejski Bank Centralny. Pierwszym aktem prawnym, który wprowadził obowiązek zapewnienia proceduralnego bezpieczeństwa podczas świadczenia usług płatniczych, była Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD1). Należy jednak zaznaczyć, że dokument ten nie zawierał szczegółowych regulacji odnoszących się bezpośrednio do cyberbezpieczeństwa.

53 Przykładowo, wzrost rentowności obligacji Skarbu Państwa przełożył się na spadek kapitałów własnych banków o około 30 mld złotych w latach 2022–2023.

Precyzyjniejsze wymogi dotyczące cyberbezpieczeństwa usług płatniczych zostały wprowadzone przez Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (PSD 2). Dokument ten nakładał na podmioty ubiegające się o zezwolenie na świadczenie usług płatniczych obowiązek opracowania strategii bezpieczeństwa oraz raportowania incydentów związanych z bezpieczeństwem. Dyrektywa wprowadza również wymóg stosowania przez dostawców usług płatniczych silnego uwierzytelniania klienta, które zostało zdefiniowane jako mechanizm uwierzytelniania dwuskładnikowego. Ponadto PSD 2 zobowiązuje Europejski Urząd Nadzoru Bankowego (EBA) do zapewnienia bezpiecznej komunikacji w ramach usług płatniczych poprzez określenie wymogów dotyczących wspólnych i otwartych standardów komunikacyjnych, które powinny zostać wdrożone przez wszystkich dostawców usług płatniczych.

Znaczący wpływ na kształtowanie regulacji wzmacniających cyberbezpieczeństwo sektora finansowego w Unii Europejskiej miało sprawozdanie „Systemic Cyber Risk" opublikowane przez Europejską Radę ds. Ryzyka Systemowego (ESRB) w lutym 2020 roku. Podkreślono w nim, że współczesny system finansowy, aby skutecznie realizować swoje podstawowe funkcje, musi opierać się na stabilnej infrastrukturze informatycznej. Naruszenie stabilności tej infrastruktury może bezpośrednio przełożyć się na zdolność systemu finansowego do pełnienia jego funkcji gospodarczych. W sprawozdaniu zwrócono uwagę, że ryzyko cybernetyczne różni się od innych rodzajów ryzyk operacyjnych przede wszystkim szybkością i skalą propagacji, a także celowym charakterem działań sprawców ataków. Co istotne, atak nie musi być bezpośrednio wymierzony w infrastrukturę systemu finansowego – może dotyczyć podmiotów ściśle z nim powiązanych, takich jak dostawcy usług w chmurze obliczeniowej. ESRB przedstawia w raporcie scenariusze, które pokazują, w jaki sposób incydent związany z cyberbezpieczeństwem może przekształcić się w kryzys systemowy, na przykład poprzez eskalację z przerwy operacyjnej do kryzysu płynnościowego, w sytuacji, gdy zaufanie do systemu finansowego zostanie podważone.

Szerokie ramy prawne mające na celu wzmocnienie cyberbezpieczeństwa kluczowych sektorów gospodarki, w tym sektora finansowego, zostały uchwalone przez Parlament Europejski i Radę pod koniec 2022 roku. Kluczowym aktem prawnym Unii Europejskiej w tym zakresie jest Dyrektywa 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS 2). Dyrektywa ta została przyjęta po rewizji wcześniejszej Dyrektywy 2016/1148, która nie zawierała wystarczająco szczegółowych regulacji dotyczących zapewnienia cyberbezpieczeństwa, co skutkowało rozbieżnościami w jej implementacji w poszczególnych państwach członkowskich UE. NIS 2 wprowadza konkretne wymagania dotyczące organizacji systemu cyberbezpieczeństwa na poziomie krajowym, zobowiązując państwa członkowskie m.in. do:

- powołania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);
- zgłaszania incydentów związanych z cyberbezpieczeństwem;
- ustanowienia punktów kontaktowych odpowiedzialnych za koordynację działań w zakresie bezpieczeństwa sieci i systemów informatycznych oraz współpracę na poziomie Unii;
- opracowania krajowych strategii cyberbezpieczeństwa, określających strategiczne cele, priorytety oraz mechanizmy zarządzania służące ich realizacji;
- promowania aktywnej cyberobrony.

Ponadto, Dyrektywa powołuje instytucje wspierające współpracę i zarządzanie kryzysowe w obszarze cyberbezpieczeństwa:

- Grupę Współpracy, której zadaniem jest wspieranie i ułatwianie wymiany informacji oraz współpracy między państwami członkowskimi;
- europejską sieć organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU-CyCLONe), odpowiedzialną za koordynację działań operacyjnych i zarządzanie incydentami oraz kryzysami cybernetycznymi na dużą skalę.

W Dyrektywie NIS 2 zwraca się również uwagę na konieczność monitorowania i promowania cyberhigieny, obejmującej podstawowy zestaw dobrych praktyk, które powinni stosować użytkownicy końcowi systemów informatycznych.

Równolegle do Dyrektywy NIS 2, Parlament Europejski i Rada przyjęły Rozporządzenie (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Akt ten zawiera bezpośrednie wytyczne dotyczące zapewnienia cyberbezpieczeństwa przez podmioty sektora finansowego, precyzując i uzupełniając wymagania określone w NIS 2. W odróżnieniu od NIS 2, która koncentruje się na ogólnych ramach organizacyjnych w zakresie cyberbezpieczeństwa, DORA wprowadza szczegółowe obowiązki dla instytucji finansowych w zakresie zarządzania ryzykiem ICT. Rozporządzenie zobowiązuje te podmioty do wdrożenia mechanizmów

zarządzania i kontroli, umożliwiających skuteczne zarządzanie wszystkimi rodzajami ryzyk związanych z infrastrukturą informacyjno-komunikacyjną. Instytucje finansowe muszą wdrożyć rozwiązania pozwalające na przewidywanie ryzyk, wczesne wykrywanie zagrożeń i incydentów ICT, ich dokumentowanie oraz zgłaszanie do właściwych organów nadzorczych – w Polsce do Komisji Nadzoru Finansowego. Co więcej, instytucje finansowe są zobowiązane do przeprowadzania testów penetracyjnych co najmniej raz na trzy lata, które mają na celu kontrolowane, oparte na analizie zagrożeń testowanie krytycznych systemów ICT.

Ważnym elementem DORA jest także promowanie współpracy międzyinstytucjonalnej. Rozporządzenie zachęca do wymiany informacji o cyberzagrożeniach pomiędzy podmiotami finansowymi, co ma na celu zwiększenie świadomości w zakresie cyberbezpieczeństwa oraz budowanie odporności operacyjnej całego sektora. DORA rozszerza też zakres odpowiedzialności instytucji finansowych w obszarze współpracy z podmiotami trzecimi. Rozporządzenie nakłada obowiązek zarządzania ryzykiem związanym z zewnętrznymi dostawcami usług ICT, proporcjonalnie do istotności tych usług oraz ich wpływu na ciągłość i dostępność usług finansowych. Ponadto ustanawia ramy nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, które sprawuje tzw. wiodący organ nadzorczy – obecnie jest nim Wspólny Komitet Europejskich Urzędów Nadzoru.

Organy Unii Europejskiej zdecydowały także o ściślejszym uregulowaniu działalności w zakresie obrotu kryptoaktywami. Kwestie związane z cyberbezpieczeństwem dostawców usług w zakresie kryptoaktywów zostały ujęte w omówionym wcześniej rozporządzeniu DORA, które nakłada na te podmioty obowiązki w zakresie zarządzania ryzykiem ICT oraz raportowania incydentów.

Uzupełnieniem działań regulacyjnych w tym obszarze jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów (MiCA), które reguluje kwestie związane z emisją, obrotem oraz wymaganiami informacyjnymi dotyczącymi kryptoaktywów. MiCA wprowadza definicje i klasyfikacje różnych typów kryptoaktywów, takich jak tokeny powiązane z aktywami, tokeny pieniądza elektronicznego oraz tokeny użytkowe, koncentrując się przy tym na ochronie inwestorów.

W ramach ochrony uczestników rynku, MiCA nakłada na emitentów obowiązek publikacji dokumentu informacyjnego dotyczącego oferowanego kryptoaktywa, wprowadza wymogi kapitałowe oraz obowiązek ochrony aktywów klientów. Warto zauważyć, że mimo szerokiego zakresu regulacji, MiCA nie obejmuje tokenów niewymienialnych (NFT), które reprezentują własność unikatowych zasobów cyfrowych lub materialnych.

Organy Unii Europejskiej regularnie dokonują przeglądu obowiązujących regulacji, dostosowując je do zmieniających się warunków technologicznych i rynkowych. Obecnie trwają prace legislacyjne nad nowym pakietem regulacyjnym obejmującym Dyrektywę Parlamentu Europejskiego i Rady w sprawie usług płatniczych i usług związanych z pieniądzem elektronicznym w ramach rynku wewnętrznego (PSD3) oraz Rozporządzenie Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego (PSR).

Projekt dyrektywy PSD3 ma na celu aktualizację dotychczasowych regulacji dotyczących usług płatniczych i pieniądza elektronicznego, zastępując obowiązujące akty prawne: Dyrektywę 2015/2366 (PSD2) oraz Dyrektywę 2009/110/WE w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością. Równolegle opracowywane rozporządzenie PSR będzie miało charakter bezpośrednio obowiązujący i skoncentruje się na relacji usługodawca–klient. W projekcie tego rozporządzenia określono szczegółowe obowiązki informacyjne wobec użytkowników usług płatniczych oraz ramy prawne dla zawieranych z nimi umów. Projekt ten przewiduje również rozszerzenie zakresu stosowania mechanizmu silnego uwierzytelniania klienta na sytuacje związane z dostępem do informacji o rachunku płatniczym. Jednocześnie uchyla ten wymóg w przypadku transakcji inicjowanych przez odbiorcę.

3.3.3. Aspekty technologiczne (cyberbezpieczeństwo, zabezpieczenia, systemy rozproszone, itp.)

Uchwalone w ostatnich latach, scharakteryzowane w podpunkcie 3.3.2. regulacje prawne Unii Europejskiej, takie jak Dyrektywa NIS2 oraz Rozporządzenie DORA, odnoszą się do technologicznych aspektów ryzyka geopolitycznego. Podmioty z sektora finansowego niewątpliwie potrzebują praktycznych wskazówek dotyczących wdrażania rozwiązań podnoszących poziom cyberbezpieczeństwa. W tym zakresie mogą korzystać z uznanych, dostępnych od lat zbiorów dobrych praktyk publikowanych przez

instytucje amerykańskie (np. NIST Cybersecurity Framework 2.0) oraz brytyjskie (np. Cyber Security Body of Knowledge – CyBOK v1.1). W ostatnich latach pojawiły się również zbiory dobrych praktyk opracowane przez instytucje Unii Europejskiej, które odpowiadają zarówno aktualnym regulacjom prawnym, jak i wyzwaniom wynikającym z rosnącego ryzyka geopolitycznego.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opublikowała w czerwcu 2025 r. przewodnik wdrożeniowy „Technical Implementation Guidance: On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures". Przewodnik ten stanowi szczegółowe wsparcie dla wdrażania środków zarządzania ryzykiem ICT zgodnych z Dyrektywą 2022/2555 (NIS2) oraz z wymaganiami technicznymi i metodycznymi określonymi w Rozporządzeniu Wykonawczym Komisji (UE) 2024/2690. Mimo że nie odnosi się ono bezpośrednio do podmiotów z sektora finansowego, kompleksowy charakter wytycznych zawartych w przewodniku sprawia, że mogą one stanowić istotne źródło dobrych praktyk również dla tego sektora. Dokument ENISA, w zgodzie z Rozporządzeniem Wykonawczym, identyfikuje trzynaście kluczowych wymagań, które powinny zostać zaadresowane w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa. Zestawienie tych wymagań wraz z ich podziałem na odpowiednie kategorie przedstawiono poniżej.

1. Polityka dotycząca bezpieczeństwa sieci i systemów informatycznych

1.1. Polityka bezpieczeństwa sieci i systemów informatycznych obejmuje m.in. podejście organizacji do zabezpieczania systemów, cele w zakresie bezpieczeństwa, funkcje i obowiązki pracowników oraz wskaźniki i środki monitorowania wdrażania polityki.

1.2. Funkcje, obowiązki i uprawnienia obejmują m.in. przypisanie odpowiedzialności, egzekwowanie zasad bezpieczeństwa ICT oraz sporządzanie sprawozdań dotyczących bezpieczeństwa ICT.

2. Polityka zarządzania ryzykiem

2.1. Ramy zarządzania ryzykiem obejmują m.in. ustalenie metodyki zarządzania ryzykiem, poziomu tolerancji ryzyka, kryteriów oceny ryzyka, sposobu identyfikacji i dokumentowania ryzyka oraz jego oceny.

2.2. Monitorowanie zgodności obejmuje m.in. przeglądy i raportowanie zgodności działań z politykami bezpieczeństwa ICT.

2.3. Niezależny przegląd bezpieczeństwa informacyjnego dotyczy przeprowadzania audytów wewnętrznych.

3. Obsługa incydentów

3.1. Polityka obsługi incydentów obejmuje m.in. określenie funkcji, obowiązków i procedur dotyczących wykrywania, analizowania, ograniczania, reagowania na incydenty, usuwania ich skutków oraz dokumentowania i zgłaszania ich w odpowiednim czasie.

3.2. Monitorowanie i rejestrowanie obejmują m.in. procedury i narzędzia umożliwiające ciągłe i automatyczne monitorowanie oraz rejestrowanie zdarzeń w systemach ICT, a także analizę rejestrów pod kątem występowania anomalii.

3.3. Zgłaszanie zdarzeń obejmuje m.in. mechanizmy umożliwiające zgłaszanie podejrzanych zdarzeń przez pracowników, dostawców i klientów.

3.4. Ocena i klasyfikacja zdarzeń obejmują m.in. określenie ich wagi oraz kwalifikację jako incydentu, z uwzględnieniem jego charakteru i poziomu dotkliwości.

3.5. Reagowanie na incydenty obejmuje m.in. procedury komunikacji z zespołami reagowania na incydenty bezpieczeństwa ICT, właściwymi organami zewnętrznymi oraz zainteresowanymi stronami wewnętrznymi i zewnętrznymi.

3.6. Przeglądy po wystąpieniu incydentu obejmują m.in. analizę przyczyn incydentów oraz wyciąganie wniosków prowadzących do poprawy poziomu cyberbezpieczeństwa.

4. Ciągłość działania i zarządzanie kryzysowe

4.1. Plan ciągłości działania i przywrócenia normalnego funkcjonowania po sytuacjach nadzwyczajnych obejmuje m.in. katalog zdarzeń wpływających na ciągłość działania, kluczowe osoby kontaktowe, kolejność przywracania działalności oraz wymagane zasoby.

4.2. Zarządzanie kopiami zapasowymi i redundancją obejmuje m.in. procedury tworzenia

kopii zapasowych, sposoby ich przechowywania, kontrole integralności oraz regularne testy odzyskiwania systemów.

4.3. Zarządzanie kryzysowe obejmuje m.in. określenie funkcji i obowiązków personelu oraz podmiotów współpracujących, środków komunikacji oraz cyklicznych testów planu zarządzania kryzysowego.

5. Bezpieczeństwo łańcucha dostaw

5.1. Polityka bezpieczeństwa łańcucha dostaw obejmuje m.in. wymogi cyberbezpieczeństwa dla dostawców i usługodawców, w tym dotyczące szkoleń, certyfikacji, weryfikacji pracowników, zgłaszania incydentów oraz prawa do przeprowadzania audytów.

5.2. Rejestr dostawców i usługodawców obejmuje m.in. wykaz produktów, usług oraz procesów ICT, a także dane kontaktowe dla każdego bezpośredniego dostawcy i usługodawcy.

6. Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych

6.1. Bezpieczeństwo w procesie nabywania usług lub produktów ICT obejmuje m.in.: wymogi bezpieczeństwa, wsparcie w całym cyklu życia, dokumentację funkcji cyberbezpieczeństwa oraz metody oceny zgodności.

6.2. Bezpieczny cykl rozwojowy obejmuje m.in.: zasady bezpiecznego rozwoju systemów ICT, analizę wymogów bezpieczeństwa, stosowanie zasad inżynierii bezpieczeństwa, stosowanie zasad bezpiecznego wytwarzania oprogramowania, testowanie bezpieczeństwa oraz aktualizację zasad rozwoju systemów ICT.

6.3. Zarządzanie konfiguracją obejmuje m.in.: dokumentowanie, wdrażanie i monitorowanie konfiguracji bezpieczeństwa sprzętu, oprogramowania, usług i sieci.

6.4. Zarządzanie zmianami, naprawy i konserwacja obejmuje m.in.: procedury kontroli zmian w systemach ICT oraz ich przegląd i aktualizację.

6.5. Testowanie bezpieczeństwa obejmuje m.in.: określenie potrzeby, zakresu i rodzaju testów bezpieczeństwa, ich realizację zgodnie z metodyką oraz działania łagodzące w przypadku naruszeń.

6.6. Zarządzanie poprawkami bezpieczeństwa obejmuje m.in.: procedury stosowania, testowania i weryfikacji poprawek zabezpieczeń.

6.7. Bezpieczeństwo sieci obejmuje m.in.: dokumentację architektury sieci, ochronę domen wewnętrznych, kontrolę dostępu, eliminację zbędnych połączeń, komunikację przez zaufane kanały oraz wdrożenie nowoczesnych protokołów.

6.8. Segmentacja sieci obejmuje m.in.: oddzielenie systemów od sieci osób trzecich, polityki dostępu, ograniczenia łączności między strefami, wdrożenie strefy zdemilitaryzowanej, separację kanałów zarządzania systemami ICT i systemów produkcyjnych oraz separację systemów produkcji usług od systemów wykorzystywanych do testowania i tworzenia kopii zapasowych.

6.9. Ochrona przed szkodliwym i niedozwolonym oprogramowaniem obejmuje m.in.: wdrożenie rozwiązań wykrywających lub zapobiegających użyciu złośliwego lub nieuprawnionego oprogramowania.

6.10. Postępowanie w przypadku podatności i ich ujawnianie obejmują m.in.: monitorowanie informacji o podatnościach, skanowanie systemów ICT pod kątem podatności na zagrożenia, usuwanie zidentyfikowanych podatności oraz wdrożenie planu łagodzenia skutków.

7. Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie

Polityki te określają m.in.: metody monitorowania, pomiaru i oceny systemów ICT, osoby odpowiedzialne za monitorowanie i pomiar środków zarządzania ryzykiem oraz harmonogram analiz i ocen wyników monitorowania i pomiarów.

8. Podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa

8.1. Podnoszenie świadomości i podstawowe praktyki cyberhigieny obejmują działania edukacyjne skierowane do pracowników, dostawców i usługodawców w zakresie identyfikacji i reagowania na cyberzagrożenia.

8.2. Szkolenia w zakresie bezpieczeństwa obejmują zapewnienie odpowiednich programów edukacyjnych dla pracowników pełniących

funkcje wymagające specjalistycznej wiedzy i umiejętności w obszarze bezpieczeństwa ICT.

9. Kryptografia

Podmioty są zobowiązane do ustanowienia, wdrożenia i stosowania polityk oraz procedur kryptograficznych w celu zapewnienia poufności, autentyczności i integralności danych.

10. Bezpieczeństwo zasobów ludzkich

10.1. Bezpieczeństwo zasobów ludzkich obejmuje budowanie świadomości wśród pracowników, w szczególności posiadających dostęp administracyjny, w zakresie ich obowiązków, funkcji oraz wpływu na bezpieczeństwo systemów ICT.

10.2. Sprawdzanie przeszłości obejmuje ustalenie kryteriów dla funkcji i stanowisk wymagających weryfikacji przeszłości osób na nich zatrudnionych.

10.3. Procedury po zmianie zatrudnienia obejmują zapisy umowne dotyczące obowiązków i odpowiedzialności w zakresie bezpieczeństwa ICT obowiązujących po ustaniu zatrudnienia, w tym klauzule poufności.

10.4. Procedura dyscyplinarna dotyczy postępowania w przypadku naruszenia polityki bezpieczeństwa sieci i systemów informatycznych.

11. Kontrola dostępu

11.1. Polityka kontroli dostępu obejmuje wdrożenie zasad logicznej i fizycznej kontroli dostępu do systemów ICT.

11.2. Zarządzanie prawami dostępu obejmuje przydzielanie, modyfikację i cofanie uprawnień, autoryzację dostępu przez uprawnione osoby, ograniczenie zakresu i czasu dostępu dla osób trzecich oraz prowadzenie rejestru przyznanych uprawnień.

11.3. Konta uprzywilejowane i konta administracji systemu obejmują silną identyfikację, procedury autoryzacji kont uprzywilejowanych i administracyjnych, tworzenie dedykowanych kont administracyjnych oraz minimalizację przywilejów związanych z administrowaniem systemami ICT.

11.4. Systemy administracji dotyczą ograniczenia ich wykorzystania wyłącznie do zarządzania systemami ICT, powinny one być logicznie odseparowane od oprogramowania użytkowego oraz chronione za pomocą uwierzytelniania i szyfrowania.

11.5. Identyfikacja obejmuje tworzenie unikalnych tożsamości przypisanych do konkretnych użytkowników, nadzór nad tożsamościami oraz logowanie działań związanych z zarządzaniem tożsamościami.

11.6. Uwierzytelnianie obejmuje wdrożenie bezpiecznych procedur i technologii zgodnych z polityką kontroli dostępu.

11.7. Uwierzytelnianie wieloskładnikowe obejmuje stosowanie wielu czynników uwierzytelniających lub mechanizmów ciągłego uwierzytelniania, dostosowanych do klasyfikacji zasobów.

12. Zarządzanie aktywami

12.1. Klasyfikacja aktywów obejmuje opracowanie systemu poziomów klauzul tajności oraz przypisanie odpowiednich klas do wszystkich aktywów.

12.2. Postępowanie z aktywami obejmuje wdrożenie polityki zarządzania aktywami w całym ich cyklu życia, w tym zasady bezpiecznego użytkowania, przechowywania, transportu i niszczenia.

12.3. Polityka dotycząca nośników wymiennych obejmuje zakaz ich podłączania (z wyjątkiem określonych przypadków), blokadę automatycznego uruchamiania programów, skanowanie pod kątem złośliwego kodu, kontrolę i ochronę urządzeń przenośnych oraz stosowanie kryptografii w celu ochrony danych.

12.4. Wykaz aktywów obejmuje listę operacji i usług wraz z ich opisem oraz listę sieci i systemów informatycznych.

12.5. Zdeponowanie, zwrot lub usunięcie aktywów po zakończeniu zatrudnienia obejmuje wdrożenie odpowiednich procedur i dokumentacji dotyczących aktywów pozostających w dyspozycji personelu.

13. Bezpieczeństwo środowiskowe i fizyczne

13.1. Usługi pomocnicze powinny zapobiegać utracie, uszkodzeniu lub przerwom w działaniu systemów poprzez ochronę przed awariami zasilania, redundancję oraz umowy na dostawy awaryjne.

13.2. Ochrona przed zagrożeniami fizycznymi i środowiskowymi obejmuje działania zapobiegające lub ograniczające skutki zdarzeń wynikających z takich zagrożeń.

13.3. Kontrola dostępu obwodowego i fizycznego obejmuje zapobieganie oraz monitorowanie nieuprawnionego fizycznego dostępu, uszkodzeń i ingerencji w systemy ICT.

Do innych istotnych dokumentów wspierających zapewnienie cyberbezpieczeństwa, opracowanych przez ENISA, należą Europejskie Ramy Umiejętności w Zakresie Cyberbezpieczeństwa (*European Cybersecurity Skills Framework* – ECSF), opublikowane w 2022 roku. Stanowią one wspólny punkt odniesienia dla definiowania i oceny kompetencji zawodowych w obszarze cyberbezpieczeństwa na poziomie Unii Europejskiej. Ramy te identyfikują 12 profili zawodowych i określają dla każdego z nich wymagane umiejętności, wiedzę oraz kompetencje.

W czerwcu 2025 roku ENISA opublikowała dokument pt. *Cybersecurity Roles and Skills for NIS2 Essential and Important Entities*, który wspomaga mapowanie zadań i odpowiedzialności określonych w Dyrektywie NIS2 na konkretne profile zawodowe zdefiniowane w ECSF.

W dokumentach opublikowanych przez ENISA brakuje szczegółowego opisu procedur związanych z przeprowadzaniem okresowych testów penetracyjnych, wymaganych na mocy rozporządzenia DORA. Lukę tę wypełnia opublikowany przez Europejski Bank Centralny model TIBER-EU (*Threat Intelligence-Based Ethical Red Teaming*), który stanowi ramy testowania odporności systemów ICT na zagrożenia, dedykowane różnym podmiotom, w tym instytucjom finansowym. TIBER-EU określa role i obowiązki uczestników testów penetracyjnych, opisuje poszczególne etapy ich realizacji oraz definiuje wymagania dotyczące dokumentacji, bezpieczeństwa i poufności. Ramy te umożliwiają ocenę zdolności organizacji do wykrywania, reagowania i przeciwdziałania realistycznym scenariuszom ataków. Ułatwia identyfikację luk w zabezpieczeniach, procesach organizacyjnych oraz zachowaniach pracowników, a także wspiera formułowanie wniosków służących doskonaleniu zarządzania ryzykiem w obszarze ICT.

3.3.4. Sposoby ograniczania ryzyka geopolitycznego – aspekty sektorowe

Oprócz aspektów regulacyjnych i odnoszących się do cyberbezpieczeństwa istotne są również działania podejmowane przez same banki w odniesieniu do poszczególnych obszarów ich funkcjonowania. Jak bowiem podkreślono w raporcie NBP (2024), z uwagi na uwarunkowania i cechy ryzyka geopolitycznego głównym sposobem radzenia sobie z nim jest budowanie odporności na poziomie indywidualnych podmiotów i całego systemu finansowego.

W tym kontekście do najważniejszych działań, które mogą i powinny podjąć instytucje finansowe (we współpracy z nadzorcami oraz innymi instytucjami wspierającymi) można zaliczyć:

1. **Ciągły monitoring** rozwoju ryzyka geopolitycznego, a także potencjalnych kanałów wpływu tego ryzyka w skali lokalnej i globalnej przez instytucje finansowe oraz instytucje tworzące *safety net*; wdrożenie systemów wczesnego ostrzegania do monitorowania wskaźników geopolitycznych.
2. **Wzmacnianie odporności** systemów finansowych na szoki (także geopolityczne) poprzez odpowiednie działania z zakresu nadzoru mikro- i makroostrożnościowego, takich jak, przykładowo, ustanawianie dodatkowych wymogów kapitałowych oraz odpowiednich zasad zarządzania ryzykiem (np. zastosowanie tzw. neutralnego antycyklicznego bufora kapitałowego (nBA) lub/i dodatkowego wymogu w zakresie funduszy własnych).
3. **Regularne testy warunków skrajnych**, mające zidentyfikować scenariusze[54], które prowadziłyby do zachwiania stabilności systemu finansowego (ang. *reverse stress tests*).
4. **Regularne przeglądy koncentracji ekspozycji** (pośrednich i bezpośrednich) na podmioty z państw o wysokim ryzyku geopolitycznym, a także względem podmiotów z branż i rynków również cechujących się wysokim poziomem tego ryzyka.

54 Przykładowe scenariusze uwzględniające rozmaite manifestacje ryzyka geopolitycznego ujęto w aneksie 1.

5. **Dywersyfikacja ekspozycji** – rozproszenie działalności na różne branże, regiony i rynki geograficzne, aby uniknąć nadmiernej koncentracji w niestabilnych obszarach; dywersyfikacja może mieć charakter geograficzny (rozpraszanie działalności na różne rynki i regiony), **sektorowy** (unikanie nadmiernej koncentracji w branżach szczególnie wrażliwych na szoki geopolityczne, takich jak, energia, surowce, transport i logistyka) oraz **walutowy** (ograniczanie niezabezpieczonej ekspozycji waluty krajów politycznie niestabilnych lub potencjalnie wrogich).

6. **Utrzymanie operacyjnej „odporności cyfrowej"** instytucji finansowych oraz zapewnienie ciągłości świadczenia usług informatycznych na rynku finansowym (w tym przez podmioty trzecie), czemu powinno służyć wdrożenie rozporządzenia DORA (zob. punkt 3.3.2), regularne testowanie przez instytucje finansowe planów awaryjnych, również na przypadki zaburzeń działania infrastruktury krytycznej, a także przygotowanie opcji migracji systemów informatycznych banków do infrastruktury chmurowej.

7. **Zabezpieczenia finansowe** – *hedging* ryzyka walutowego, stóp procentowych czy cen surowców za pomocą instrumentów pochodnych; ubezpieczenia – polisy chroniące przed ryzykiem politycznym, w tym ryzykiem wywłaszczenia czy niemożności transferu środków; gwarancje eksportowe; utrzymywanie odpowiedniego poziomu rezerw w różnych walutach, co może zabezpieczyć przed nagłymi wahaniami kursów wywołanymi wydarzeniami geopolitycznymi.

8. **Planowanie ciągłości biznesowej** – opracowanie planów awaryjnych na wypadek eskalacji konfliktów geopolitycznych, w tym procedur ewakuacji personelu, zabezpieczenia danych i utrzymania kluczowych operacji.

9. **Lokalne partnerstwa strategiczne** – współpraca z lokalnymi instytucjami finansowymi może zapewnić lepsze zrozumienie lokalnego otoczenia politycznego i dostęp do informacji o potencjalnych zagrożeniach.

10. **Utrzymywanie „konserwatywnego" (tradycyjnego) modelu biznesowego**[55] (duża rola tradycyjnej działalności kredytowo-depozytowej, szczególnie w segmencie detalicznym, ograniczona rola działalności inwestycyjnej; stosunkowo wysokie wymogi wobec kredytobiorców, koncentracja na rynku krajowym, ostrożne podejście do instrumentów inżynierii finansowej).

11. **Zapewnienie, przy kluczowej roli banku centralnego – w kontekście rozważań z punktu 2.5 – odpowiedniego zapasu rezerw gotówkowych, dostępu do gotówki, niezakłóconego obrotu gotówkowego oraz odpowiednich procedur awaryjnych w tym zakresie**, w tym przede wszystkim:
    - zapewnienie wystarczających zapasów gotówki i zdolności jej produkcji (najlepiej ulokowanych w kraju na wypadek kryzysu);
    - zdywersyfikowane geograficznie rozmieszczenie punktów dystrybucji gotówki;
    - zdywersyfikowanie struktury podmiotów zajmujących się transportem gotówki;
    - wspieranie polityki dostępu do gotówki oraz jej komplementarności z cyfrowymi środkami płatniczymi;
    - współpracę banków komercyjnych z bankiem centralnym w zakresie edukacji monetarnej, uwzględniającej geopolityczny kontekst funkcjonowania gotówki.

W odniesieniu do kwestii gotówkowych można jednak zaobserwować pewną **różnicę perspektyw** banków komercyjnych i władz. Mianowicie, z punktu widzenia banków redukcja infrastruktury gotówkowej (placówki, bankomaty, transport) jest elementem optymalizacji kosztowej. Stanowi to działanie racjonalne z punktu widzenia pojedynczej instytucji w „spokojnych" czasach. Decyzje o infrastrukturze gotówkowej mogą być podejmowane z myślą o optymalizacji portfela, nie zaś o odporności systemowej. Bank centralny, jako podmiot organizujący obieg gotówkowy i zainteresowany jego sprawnym funkcjonowaniem, musi jednak brać pod uwagę także szerszą perspektywę.

Pojawia się tu zatem problem pogodzenia **logiki i racjonalności mikroekonomicznej z wymogami stabilności systemowej i koniecznością zapewnienia bezpieczeństwa infrastruktury krytycznej w obszarze gotówki**. Rozwiązanie tego problemu leży niewątpliwie w interesie wszystkich stron i wymaga aktywnej roli państwa. Nasuwającym się tu rozwiązaniem jest **redundancja rozwiązań** w zakresie rozmaitych instrumentów i form płatności, gotówkowych i bezgotówkowych, czego dowodzą choćby problemy, jakie towarzyszą (czasowym) awariom systemów transakcyjnych czy aplikacji pojedynczych banków. Nawet w takim przypadku skala niedogodności i towarzyszące temu koszty są znaczące. Gdyby zaś problem miał charakter systemowy, konsekwencje byłyby już bardzo poważne.

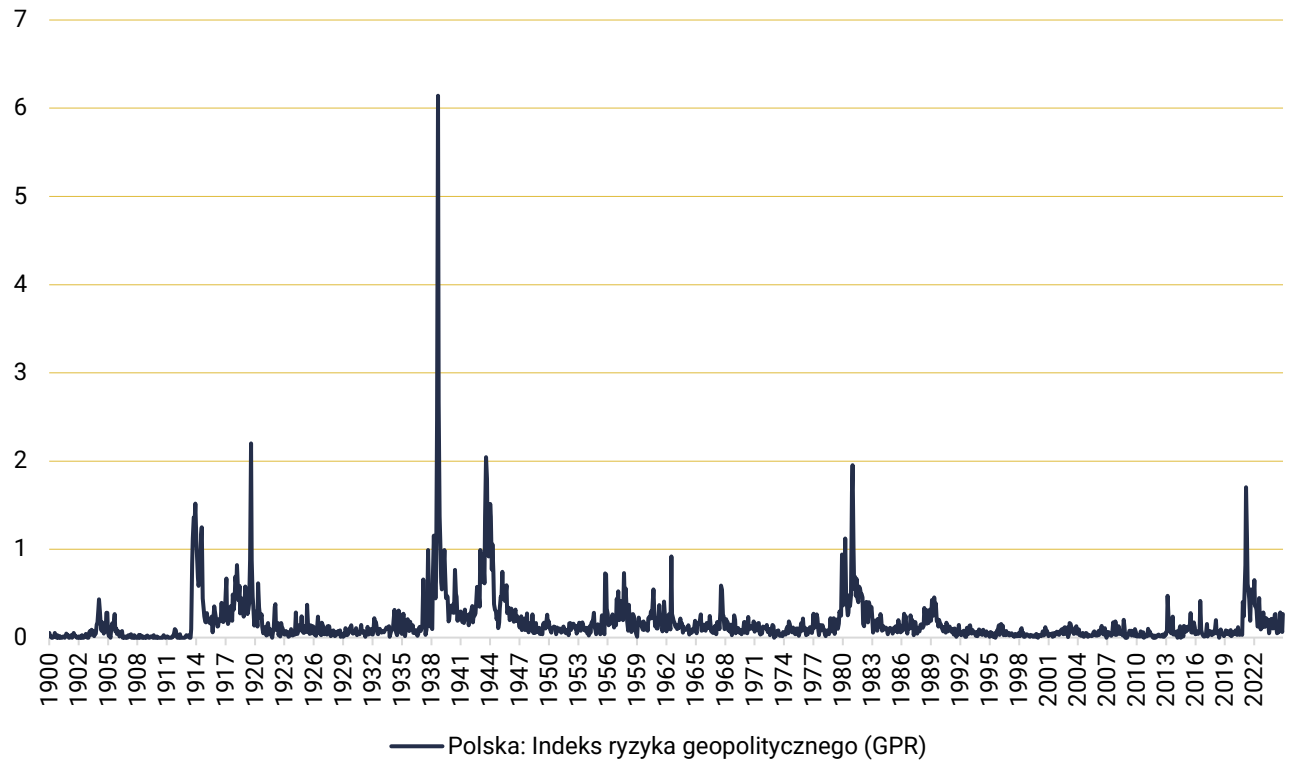
55 Oczywiście, należy tu jednak pamiętać o ujemnych stronach takiego podejścia.

Część 4. Polski system bankowy w kontekście ryzyka geopolitycznego w Polsce – wybrane aspekty

4.1. Występowanie i nasilenie ryzyka geopolitycznego w Polsce

Niezależnie od aspektów globalnych, szczególną uwagę w kontekście celu niniejszego opracowania należy zwrócić na kształtowanie się ryzyka geopolitycznego w odniesieniu do Polski. Niewątpliwie nasz kraj, z uwagi głównie na uwarunkowania historyczne, jest raczej „biorcą", niż generatorem ryzyka tego typu. Używając terminologii gier niekooperacyjnych, można uznać, iż Polska jest naśladowcą (ang. *follower*), który reaguje na ryzyko geopolityczne generowane przez ważniejszych (z różnych względów) graczy, nie zaś liderem, podmiotem wyznaczającym kierunki i obszary problemowe. W tym ujęciu, ryzyko geopolityczne jest dla naszej gospodarki i składających się na nią podmiotów (w tym banków) zmienną egzogeniczną. Oczywiście, możliwe jest do pewnego stopnia (w zależności od prezentowanej sprawczości) redukowanie źródeł i stopnia tego ryzyka[56], jednak podejmowane działania mają tu przede wszystkim charakter dostosowań, mających na celu ograniczanie negatywnych konsekwencji materializacji poszczególnych rodzajów ryzyka geopolitycznego, wraz z towarzyszącymi im kosztami i problemami.

Wykres 10. Ryzyko geopolityczne w Polsce w latach 1900–2025



Źródło: Opracowanie własne na podstawie Geopolitical Risk Index.

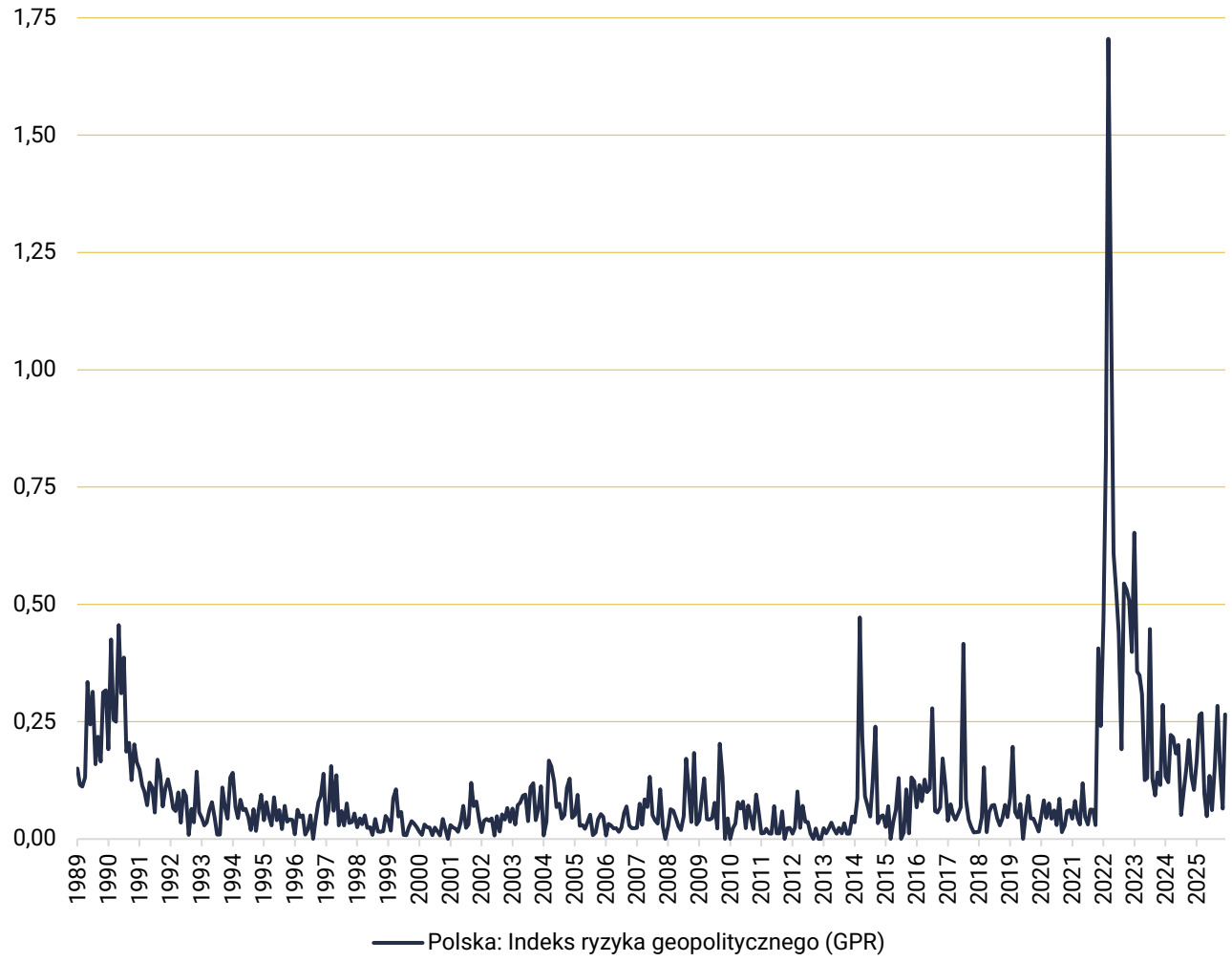
Na Wykresie 10. przedstawiono zmiany indeksu ryzyka geopolitycznego (GPR) dla Polski w latach 1900–2025. Polska, ze względu na swoje położenie geopolityczne w Europie Środkowo-Wschodniej, była i pozostaje szczególnie narażona na wahania poziomu ryzyka geopolitycznego. Wykres ukazuje wyraźne wzrosty indeksu w okresach największych wstrząsów historycznych: I wojny światowej (1914–1918), II wojny światowej (1939–1945), a także w czasie zimnej wojny, kiedy Polska znajdowała się w strefie wpływów ZSRR. Wysokie wartości indeksu odnotowano również w okresie transformacji ustrojowej po 1989 roku, co odzwierciedlało niepewność polityczną i społeczną związaną z przejściem od sys-

56 Spektakularnym tego wyrazem jest, jak się wydaje, reakcja Polski na rosyjską napaść na Ukrainę.

temu komunistycznego do demokracji i gospodarki rynkowej oraz następstwami tego procesu.

W ostatnich dwóch dekadach indeks ryzyka geopolitycznego dla Polski wykazuje istotne wahania, szczególnie w latach 2014 (aneksja Krymu przez Rosję), 2020 (pandemia COVID-19) oraz 2022 (pełnoskalowa inwazja Rosji na Ukrainę). Wzrosty te są wynikiem zarówno bezpośrednich zagrożeń w regionie, jak i ogólnego wzrostu napięć międzynarodowych, w których Polska – jako członek NATO i Unii Europejskiej – odgrywa istotną rolę.

Wykres 11. Ryzyko geopolityczne w Polsce w latach 1989–2025

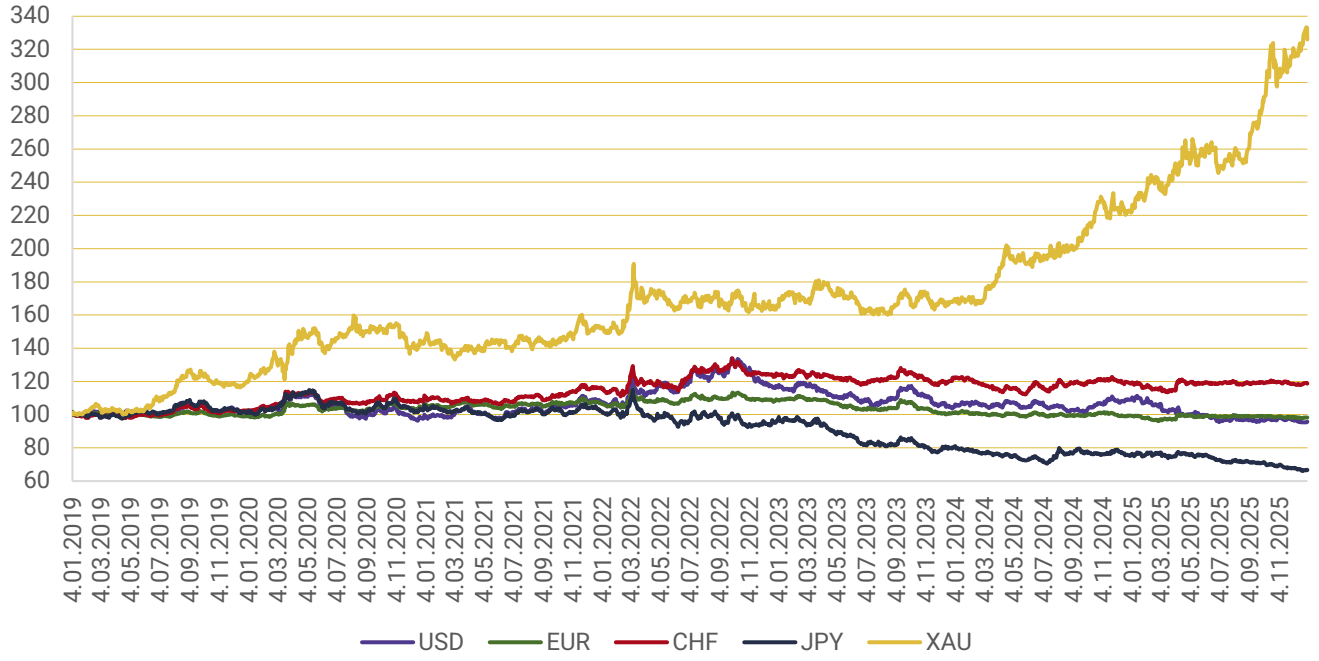


Źródło: Opracowanie własne na podstawie Geopolitical Risk Index.

Dla lepszego zobrazowania najnowszych tendencji i wyzwań w zakresie ryzyka geopolitycznego sporządzono dodatkowo Wykres 11. Koncentruje się on na okresie po 1989 roku, umożliwiając bardziej szczegółową analizę bieżących trendów. Z wykresu wynika, że mimo ogólnej stabilizacji politycznej i gospodarczej po wejściu Polski do NATO (1999) i Unii Europejskiej (2004), poziom ryzyka geopolitycznego nadal cechuje się zmiennością. Szczególnie istotne są skoki indeksu w latach 2014 i 2022, które pokazują, że Polska – mimo integracji z Zachodem – nadal znajduje się w strefie podwyższonego ryzyka związanego z bliskością konfliktów zbrojnych i napięć międzynarodowych.

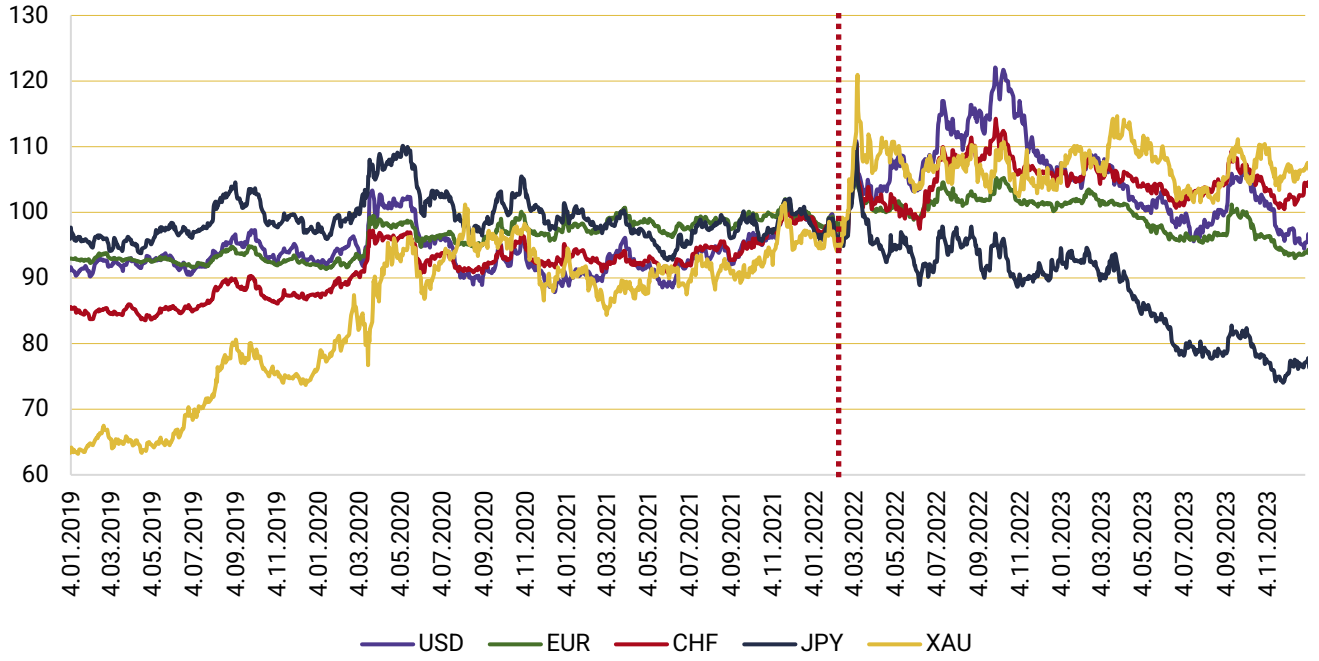
Niezależnie od tych syntetycznych mierników, wzrost ryzyka geopolitycznego w odniesieniu do naszej gospodarki można zaobserwować również obserwując kształtowanie się indeksów kursów głównych walut oraz złota (wykresy 12–13) Podobnie jak wcześniej dla kryptowalut, przyjęto tutaj dwie perspektywy: ujęcie ogólne (indeksy jednopodstawowe, 02.2019=100) oraz *event-study*, żeby pokazać, jak w krótszym horyzoncie czasowym na rozpatrywane kategorie wpłynął wybuch wojny „pełnoskalowej" 24.02.2022 r. (indeks jednopodstawowy, gdzie 24.02.2022=100).

Wykres 12. Indeks kursów walut i złota – ujęcie ogólne (01.2019=100)



Źródło: Opracowanie własne.

Wykres 13. Indeks kursów walut i złota – event study (24.02.2022=100)



Źródło: Opracowanie własne.

Zaprezentowane wykresy potwierdzają, że Polska jest krajem wrażliwym na zmiany w regionalnym i globalnym układzie sił, a wydarzeniem przełomowym w tym zakresie była oczywiście rosyjska inwazja na Ukrainę. Potwierdzają również tezę, iż jesteśmy raczej „biorcą" ryzyka, mimo udziału w międzynarodowych organizacjach i stowarzyszeniach. To ostatnie, oczywiście (jak zostanie to rozwinięte w dalszej części raportu), obniża ekspozycję na ryzyko geopolityczne, ale nie chroni przed nim całkowicie[57].

57 Paradoksalnie, w niektórych przypadkach może je nawet zwiększyć. Przykładem jest tu słynny art. 5 NATO, zgodnie z którym, jeśli takie byłyby ustalenia, Polska powinna zareagować na agresję wobec innego kraju natowskiego.

Ostatnie lata przyniosły znaczący wzrost ryzyka geopolitycznego dla Polski, a tym samym – także dla polskiego systemu bankowego. Wśród najważniejszych źródeł tego ryzyka można wymienić przede wszystkim:

1. **Konflikt w Ukrainie i bezpieczeństwo regionalne.** Wojna w Ukrainie pozostaje największym bezpośrednim zagrożeniem. Może wpłynąć na stabilność finansową regionu, wywołać dalsze fale uchodźców generujące koszty społeczne, oraz prowadzić do zwiększonych wydatków obronnych obciążających budżet państwa. Niewykluczona jest także dalsza eskalacja konfliktu, która może dodatkowo zakłócić handel, łańcuchy dostaw, a także rozszerzyć się o działania poniżej progu wojny kinetycznej, ale mające już znamiona wojny hybrydowej (np. atak rosyjskich dronów w nocy z 9 na 10 września 2025, sytuacja na granicy białoruskiej).

2. **Relacje z Rosją i sankcje.** Przedłużające się sankcje wobec Rosji wpływają na polskie banki przez ograniczenia w handlu i inwestycjach. Istnieje ryzyko dalszego zaostrzenia sankcji lub rosyjskich działań odwetowych, które mogą dotknąć polskie instytucje finansowe, mające jeszcze jakiekolwiek powiązania z rynkiem rosyjskim (oraz białoruskim).

3. **Zmiany w polityce UE i strefa euro.** Zmiany w polityce fiskalnej i monetarnej UE (zmiany celów, instrumentów, zasad funkcjonowania), a także perspektywa potencjalnej integracji polskiej gospodarki ze strefą euro mogą wpłynąć na polskie banki.

4. **Relacje transatlantyckie.** Zmiany w polityce USA wobec Europy Środkowej mogą wpłynąć na przepływy kapitału i inwestycje amerykańskie w polskim sektorze bankowym. Polityka handlowa USA również może oddziaływać na polską gospodarkę, zarówno samą w sobie, jak i część UE.

5. **Napięcia z Chinami.** Rosnące napięcia geopolityczne między Zachodem a Chinami mogą wpłynąć na gospodarcze relacje między Polską a Państwem Środka[58]; polskie banki obsługujące handel z Azją mogą natrafić na mniej sprzyjające warunki, ograniczeniu może też ulec dostęp do chińskich inwestycji i technologii.

6. **Ryzyko cybernetyczne.** Zwiększone zagrożenia cybernetyczne ze strony państw wrogich, szczególnie w kontekście konfliktu w Ukrainie, stanowią poważne ryzyko dla infrastruktury bankowej.

7. **Konflikty w innych częściach świata.** Rosnące napięcia w wielu regionach świata (Iran, Izrael, Pakistan) zmieniają ceny importowanych przez Polskę surowców (w tym ropy naftowej), oddziałują na ogólną niestabilność i stopień zaangażowania głównych podmiotów.

4.2. Swoiste cechy polskiego systemu bankowego w kontekście ryzyka geopolitycznego

W kontekście tak poważnych i zróżnicowanych zagrożeń dla stabilności i rozwoju państwa polskiego i polskiej gospodarki pojawia się pytanie, na ile polski system bankowy jest podatny na poszczególne formy ryzyka geopolitycznego, a na ile dysponuje cechami oraz mechanizmami obronnymi, chroniącymi go przed materializacją ryzyka geopolitycznego wraz z wszystkimi opisanymi negatywnymi następstwami. I tak, w szczególności warto zwrócić uwagę na pewne ogólne charakterystyki:

(1) Jeżeli chodzi o **strukturę własnościową polskiego systemu bankowego** oraz jej implikacje geopolityczne, należy wskazać w pierwszej kolejności na wysoki udział kapitału zagranicznego. Zgodnie z opisanymi kanałami transmisji ryzyka geopolitycznego, czynnik taki zasadniczo postrzega się jako zwiększający podatność danego systemu bankowego na to ryzyko: sankcje lub napięcia dotyczące krajów macierzystych mogą wpływać na dostęp banków do finansowania i linii kredytowych od spółek-matek; może też potencjalnie wystąpić *contagion effect*. Niemniej, ważnym, by nie rzec kluczowym, czynnikiem jest tu struktura tego kapitału – ryzyko geopolityczne jest wyższe, jeżeli udziałowcy (właściciele) krajowych banków pochodzą z krajów rywalizujących, zaliczanych do przeciwstawnych obozów lub posiadających rozbieżne interesy geopolityczne. Nie jest to jednak przypadek Polski – kapitał zagraniczny w polskim systemie bankowym pochodzi w zasadzie prawie w całości z krajów „sojuszniczych" (głównie z UE)[59]. Nie tylko nie zwiększa to ryzyka geopolitycznego, ale wręcz je mityguje, albowiem

58 Przykładem może tu być zamknięcie granicy białorusko-polskiej, ograniczające tranzyt chińskich towarów via Małaszewicze we wrześniu 2025 r.

59 Jest on przy tym rozproszony, co również jest czynnikiem ograniczającym ryzyko geopolityczne związane z tym czynnikiem.

ewentualny atak na Polskę uderza również w interesy tych banków i tych państw, które na naszym rynku funkcjonują.

(2) Typowa dla polskiego rynku bankowego jest jego **segmentacja** – wyraźny jest podział na banki komercyjne, w których w ostatnich latach wzrosło znaczenie kapitału krajowego, przy zróżnicowanym geograficznie kapitale zagranicznym, oraz sektor spółdzielczy; specjalne miejsce w sektorze zajmują przy tym PKO BP – z uwagi na uwarunkowania historyczne, skalę działalności oraz silne powiązanie ze Skarbem Państwa – oraz BGK jako bank państwowy. Ta fragmentacja oznacza różną ekspozycję na poszczególne rodzaje ryzyka geopolitycznego, zgodnie z mechanizmami opisanymi w punkcie 3.1.

(3) W odniesieniu do **specyfiki operacyjnej** polskich banków można wskazać na ciągle obecny (choć zmniejszający się) problem kredytów frankowych; portfel kredytów walutowych (głównie CHF) w polskich bankach stanowi unikalną cechę, która czyni je wrażliwymi na gwałtowne wahania kursowe spowodowane napięciami geopolitycznymi. Ponadto polskie banki mają stosunkowo wysoką ekspozycję kredytową na małe i średnie przedsiębiorstwa, a więc podmioty, które są szczególnie wrażliwe na szoki energetyczne i problemy w funkcjonowaniu łańcuchów dostaw.

(4) Jeżeli chodzi o **koncentrację geograficzną**, polskie banki działają głównie na terytorium krajowym; ich ekspansja zagraniczna (poza nielicznymi wyjątkami, jak działalność niektórych banków w regionie) zawsze była raczej znikoma[60]. To oznacza całkowitą ekspozycję w zasadzie tylko na ryzyko krajowe bez dywersyfikacji geograficznej.

(5) Za bardzo pozytywną cechę polskiej bankowości można uznać **relatywnie wysoki poziom cyfryzacji**. Polskie banki są stosunkowo zaawansowane technologicznie (wysoki poziom bankowości mobilnej i internetowej), co zresztą jest z zadowoleniem witane przez klientów bankowych, przyzwyczajonych już do wysokiego standardu polskich podmiotów w tym zakresie. Należy jednak podkreślić, iż paradoksalnie zwiększa to ryzyko cyberataków – większa jest po prostu przestrzeń do tego typu działań (zob. Tabela 5). Ponadto wiele kluczowych systemów bankowych opiera się na rozwiązaniach zagranicznych dostawców, co tworzy potencjalną słabość w scenariuszu eskalacji napięć geopolitycznych (zob. Aneks). Cyfryzacja sprawia przy tym, że systematycznie maleje sieć fizycznych oddziałów i bankomatów, na co należy zwrócić uwagę, organizując zapewnienie podmiotom gospodarującym dostępu do gotówki.

Tabela 4. Przykłady cyberataków wymierzonych w polskie banki – 2025

Data	Opis
Wrzesień 2025	Kampanie phishingowe wobec PKO BP – hakerzy podszywali się pod PKO BP na portalach społecznościowych, publikując reklamy obiecujące nagrody. Ich celem było wyłudzenie danych logowania do bankowości elektronicznej oraz danych kart płatności.
Maj 2025	Prorosyjskie grupy hakerskie NoName057 (16) i Dark Storm przeprowadziły ataki na Wytwórnię Papierów Wartościowych, Stowarzyszenie Emitentów Giełdowych, Energę, PARP oraz operatora Play. Zaatakowane zostały również lotniska w Gdańsku i Poznaniu oraz Nest Bank.
Luty 2025	Na platformie Docer.pl ujawniono dokumenty zawierające dane klientów polskich banków, w tym wykazy operacji, nazwiska i adresy; źródłem wycieku mogła być firma księgowa lub biuro rachunkowe.
12 stycznia 2025	EuroCert, lider w dziedzinie certyfikatów elektronicznych, stał się celem ransomware. Hakerzy zaszyfrowali pliki na serwerach firmy, potencjalnie naruszając dane osobowe, w tym numery PESEL, serie dowodów osobistych i hasła
Sierpień 2023 (kontynuowane w 2025)	Prorosyjska grupa hakerska NoName057 (16) przeprowadziła ataki DDoS na Giełdę Papierów Wartościowych oraz serwisy internetowe PKO, Raiffeisen, Plus Banku, BNP Paribas, Banku Spółdzielczego w Brodnicy, Credit Agricole Polska i Santander Bank Polska.

Źródło: *Opracowanie własne na podstawie danych GUS (2025b).*

(6) Jeśli chodzi o ramy instytucjonalne funkcjonowania polskich banków, można uznać, iż były (i są) one właściwie skonstruowane i funkcjonują skutecznie na przestrzeni całego okresu po rozpoczęciu transformacji. Polska była krajem, w którym nie wystąpił kryzys bankowy, co niewątpliwie można zawdzięczać m.in. **wysokiej jakości instytucji okołobankowych**. Współcześnie, jak się

60 Rzutowało to na niski poziom internacjonalizacji polskiego systemu bankowego (zob. Marszałek i Jurek, 2010).

wydaje, Komisja Nadzoru Finansowego prowadzi stosunkowo ostrożną i konserwatywną politykę nadzorczą[61], co z jednej strony buduje odporność sektora, ale z drugiej może ograniczać elastyczność w reagowaniu na szoki. Czynnikiem zwiększającym bezpieczeństwo jest także sukcesywna, kompleksowa implementacja regulacji unijnych. Polska specyfika polega przy tym na często nawet bardziej restrykcyjnej implementacji dyrektyw UE (tzw. *gold-plating* – zob. Kaczor 2022). Zwiększa to wprawdzie obciążenia *compliance*, ale tworzy jednocześnie dodatkowy bufor regulacyjny.

(7) **Stosunkowo duża jest wrażliwość na politykę fiskalną i monetarną** (np. wakacje kredytowe, podatek bankowy i jego konstrukcja, wyższa stawka CIT dla banków – stawka 30% od 2026 r.); decyzje w zakresie *policy mix* mogą być podejmowane w reakcji na napięcia geopolityczne, tworząc dodatkowy kanał transmisji wpływu na system finansowy, co jednak może być czynnikiem raczej destabilizującym. Jak się wydaje, nadmierne i niekorzystne z punktu widzenia rozwoju banków i kształtowania się ich struktury bilansowej rozwiązania fiskalne, nastawione głównie na generowanie bieżących wpływów budżetowych, są działaniami generującymi dla decydentów korzyści doraźne, kosztem przyszłych. W dłuższej perspektywie, presja fiskalna ogranicza rozwój instytucji bankowych, a tym samym niweluje korzyści, jakie większy i silniejszy kapitałowo system mógłby kreować dla sfery realnej. Dodatkowo, tworzy ona trwałą nierównowagę, czy wręcz asymetrię rynkową, która w dłuższej perspektywie może obniżyć konkurencyjność sektora bankowego zarówno na poziomie krajowym, jak i międzynarodowym.

(8) Typowy dla polskiego sektora bankowego jest **bardzo wysoki, dominujący udział depozytów** gospodarstw domowych w finansowaniu banków. W kontekście kanałów wpływu ryzyka geopolitycznego może to powodować podatność i wrażliwość na nastroje społeczne oraz potencjalnie zwiększać ryzyko paniki bankowej w scenariuszu kryzysu wywołanego napięciami geopolitycznymi (np. w warunkach sterowanej w ramach wojny hybrydowej kampanii czarnego PR czy dezinformacji). Dodatkowo mniejsze polskie banki mają ograniczone możliwości dywersyfikacji źródeł finansowania poprzez rynki kapitałowe, co zwiększa zależność od rynku międzybankowego i finansowania od spółek-matek. Z drugiej jednak strony, należy wskazać na pozytywną, zwiększającą stabilność systemu, rolę „osadu" depozytowego, typowego dla polskich banków. Ponadto, ważnym czynnikiem także wpływającym pozytywnie na stabilność depozytów jest ich duże rozdrobnienie podmiotowe oraz wysoki udział środków gwarantowanych – oba czynniki sprawiają, że depozyty są w mniejszym stopniu podatne na masowe odpływy.

(9) **Specyfika behawioralna i kulturowa polskich banków oraz ich klientów.** Składają się na nią doświadczenia transformacji, burzliwych pierwszych lat reform, stopniowego rozwoju systemu czy wreszcie integracji z UE. Wszystko to kreuje swoiste postawy zarówno banków, jak i ich klientów w obliczu niepewności geopolitycznej. Warto jednak podkreślić, że mimo różnych percepcji instytucji bankowych i pewnych kryzysów wizerunkowych opinia o polskich bankach uległa znacznej poprawie w 2024 roku. Badanie „Reputacja polskiego sektora bankowego 2024" zrealizowane przez pracownię Minds & Roses na zlecenie Związku Banków Polskich pokazuje, że aż 54% respondentów (wzrost o 9 pkt proc. w porównaniu z rokiem 2023) wyrażało pozytywną opinię o sektorze bankowym.

(10) Z raportów i opracowań dotyczących polskiego systemu bankowego (zob. NBP 2024, 2025, ZBP 2025, BFG 2025, KNF 2025) wynika, że jest on stabilny. Ryzyko systemowe w krajowym systemie nie tylko bankowym, ale i finansowym pozostaje ograniczone. Bardzo pozytywnie można ocenić zarówno spełnianie wymogów kapitałowych, jak i rentowność polskich banków (rekordowe zyski w 2024 i 2025 roku). Bardzo niekorzystnym, patologicznym wręcz zjawiskiem jest natomiast istniejąca od stycznia 2025 sytuacja, w której polski sektor bankowy ma więcej instrumentów dłużnych (głównie Skarbu Państwa) niż kredytów, co jest ewenementem na skalę europejską i światową. Od początku 2020 r. przyrost wartości instrumentów dłużnych w polskim sektorze bankowym wyniósł 808,9 mld PLN, obligacji skarbowych o 359,9 mld PLN, obligacji gwarantowanych przez Skarb Państwa o 98,4 mld PLN, a bonów pieniężnych NBP – o 228 mld PLN. W analogicznym okresie wartość kredytów dla sektora niefinansowego zwiększyła się jedynie o 161,2 mld PLN. Oznacza to, że w ciągu ostatnich pięciu lat portfel instrumentów dłużnych wzrósł ponad pięć razy bardziej niż portfel kredytów dla sektora niefinansowego. W samym 2025 r. wartość instrumentów dłużnych zwiększyła się o 158 mld PLN, natomiast portfel kredytów dla sektora niefinansowego wzrósł o 78 mld zł, co w przybliżeniu stanowi prawie

61 Wyrazem tego jest choćby jej stanowisko względem kryptoaktywów.

dwukrotnie mniejszą wartość (PAB WIB, 2026). Obok malejącego udziału banków w finansowaniu procesów gospodarczych, tak duży udział dłużnych instrumentów skarbowych rzutuje negatywnie na kapitały banków (Pawlonka, 2025). Można to również postrzegać jako swoisty przejaw finansyzacji gospodarki – pieniądz krąży niejako wewnątrz systemu finansowego, nie dochodząc do sfery realnej i przedsiębiorstw niefinansowych.

Mając na względzie powyższe charakterystyki, należy stwierdzić, iż pozycja polskiego systemu bankowego w kontekście ryzyka geopolitycznego **pozostaje dość specyficzna**. Polski sektor bankowy pozostaje jednym z mniejszych w UE (relacja kapitału własnego do PKB plasuje Polskę na przedostatnim miejscu w UE). Niemniej, jest on tzw. „małym gigantem", o znaczącej roli regionalnej i – mimo wszystko – istotnej pozycji strategicznej[62]. Wynika to z kilku kwestii. **Po pierwsze**, jest on swoistą „bramą" do całego regionu Europy Środkowej i Wschodniej. Choć polski sektor jest stosunkowo mały w relacji do PKB, Polska jest największą gospodarką w regionie Europy Środkowo-Wschodniej. Ewentualna destabilizacja polskiego sektora bankowego mogłaby uruchomić efekt domina na cały region przez powiązania własnościowe (te same grupy działają w całym regionie), kanały handlowe i łańcuchy dostaw oraz względy psychologiczne.

Po drugie, pojawia się kwestia finansowania bezpieczeństwa i obrony. Polska w ostatnich latach zwiększa wydatki obronne (do 4% PKB), co wymaga bardzo dużego finansowania[63]. Sektor bankowy pełni tu kluczową rolę w finansowaniu kontraktów zbrojeniowych, kredytowaniu przemysłu zbrojeniowego oraz obsłudze przepływów pieniężnych związanych z obecnością sił NATO. Destabilizacja sektora bezpośrednio uderzyłaby w zdolność Polski do umacniania swojej armii, a tym samym całej wschodniej flanki NATO.

Po trzecie, polski system bankowy dominuje w regionie pod względem nowych technologii i rozwoju bankowości cyfrowej. W latach 2004–2024 polski sektor bankowy zanotował istny skok technologiczny, stając się jednym z najnowocześniejszych sektorów bankowych na świecie[64]. Polskie rozwiązania (BLIK, infrastruktura cyfrowa) są eksportowane i kopiowane w regionie[65]. W tej sytuacji, sukces cyberataku na polskie banki podważyłby zaufanie do cyfryzacji w całym regionie, spowolniłby adopcję innowacji finansowych, a także stworzyłby precedens i ułatwił cyberataki na inne kraje.

Po czwarte, wskazana wada strukturalna, czyli przewaga w portfelach polskich banków instrumentów dłużnych zamiast kredytów, oprócz negatywnych następstw dla poszczególnych banków i zaopatrzenia gospodarki w środki finansowe, ma też znaczenie systemowe. Mianowicie, wzrost rentowności obligacji Skarbu Państwa mógłby w obecnej sytuacji spowodować destabilizację systemu bankowego, problemy z wartością złotego oraz konieczność zapobiegania nie tylko kryzysowi bankowemu, ale i kryzysowi zadłużenia jednocześnie (zob. szerzej Narodowy Bank Polski, 2025a).

Reasumując, polski sektor bankowy **ma solidną pozycję kapitałową i płynnościową**, niemniej cechuje go wyraźna podatność na ryzyko geopolityczne. Wynika to z kombinacji następujących czynników, których znaczenie wzrosło w ostatnich latach.: bliskości geograficznej do konfliktów (szczególnie Ukrainy) oraz wrogich krajów (Rosji i w pewnym stopniu także Białorusi), a także wysokiej ekspozycji na obligacje skarbowe oraz nieoptymalnego policy mix. Większa wrażliwość na czynniki geopolityczne znajduje odzwierciedlenie m.in. w kształtowaniu się rentowności obligacji (wykresy 14–17), indeksów giełdowych (wykresy 18–20) oraz kontraktów terminowych i stawki WIBOR3M (wykresy 21–24). Przedstawiając te kategorie, ponownie zastosowano podejścia: ogólne, gdzie podstawą jest 2019 r., oraz tzw. *event study* – gdzie podstawą indeksu jest data agresji.

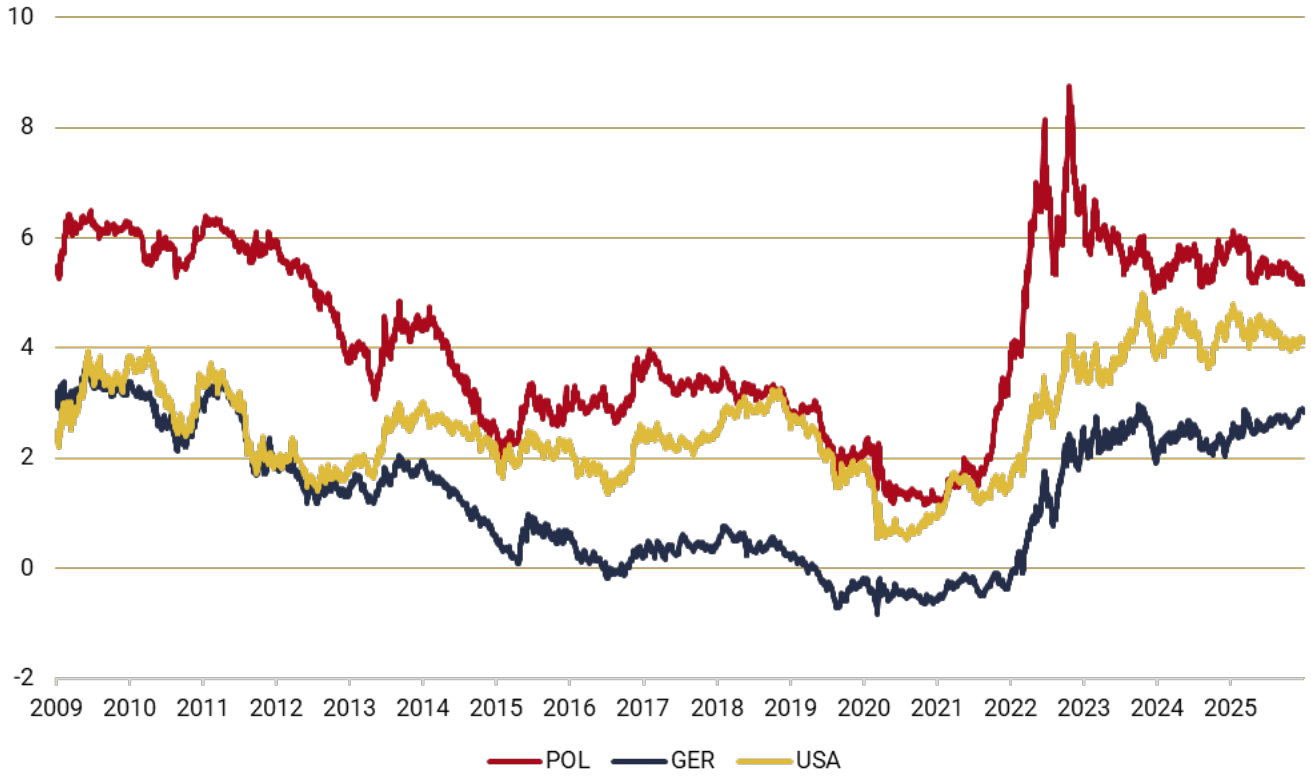
62 Potwierdzeniem takiego statusu może być m.in. wskazanie Polski wśród liderów bankowości w raporcie Deloitte „Digital Banking Maturity 2024" (https://www.deloitte.com/pl/pl/Industries/banking-capital-markets/research/Digital-Banking-Maturity-2024.html).

63 Sprawa ta jest przedmiotem rozważań w dalszej części opracowania.

64 Kwestie te są bardzo szczegółowo opisane m.in. w publikowanych dwa razy w roku raportach NBP dotyczących funkcjonowania polskiego systemu płatniczego oraz kwartalnych raportach Związku Banków Polskich „NetB@nk" dotyczących zagadnień bankowości elektronicznej, płatności bezgotówkowych.

65 Między innymi w Rumunii i Słowacji.

Wykres 14. Rentowność 10-letnich obligacji skarbowych w latach 2009–2025

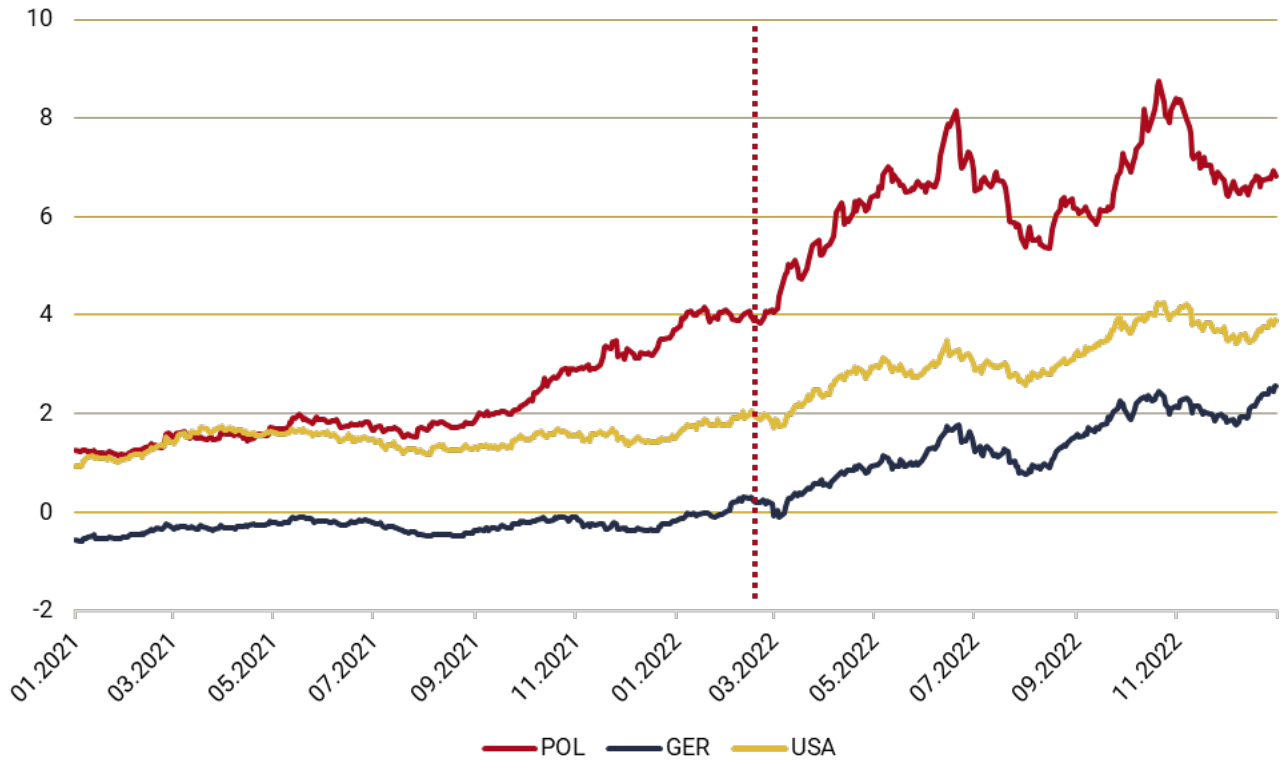


Źródło: Opracowanie własne.

Wykres 15. Różnice w rentowności 10-letnich obligacji skarbowych w latach 2009–2025

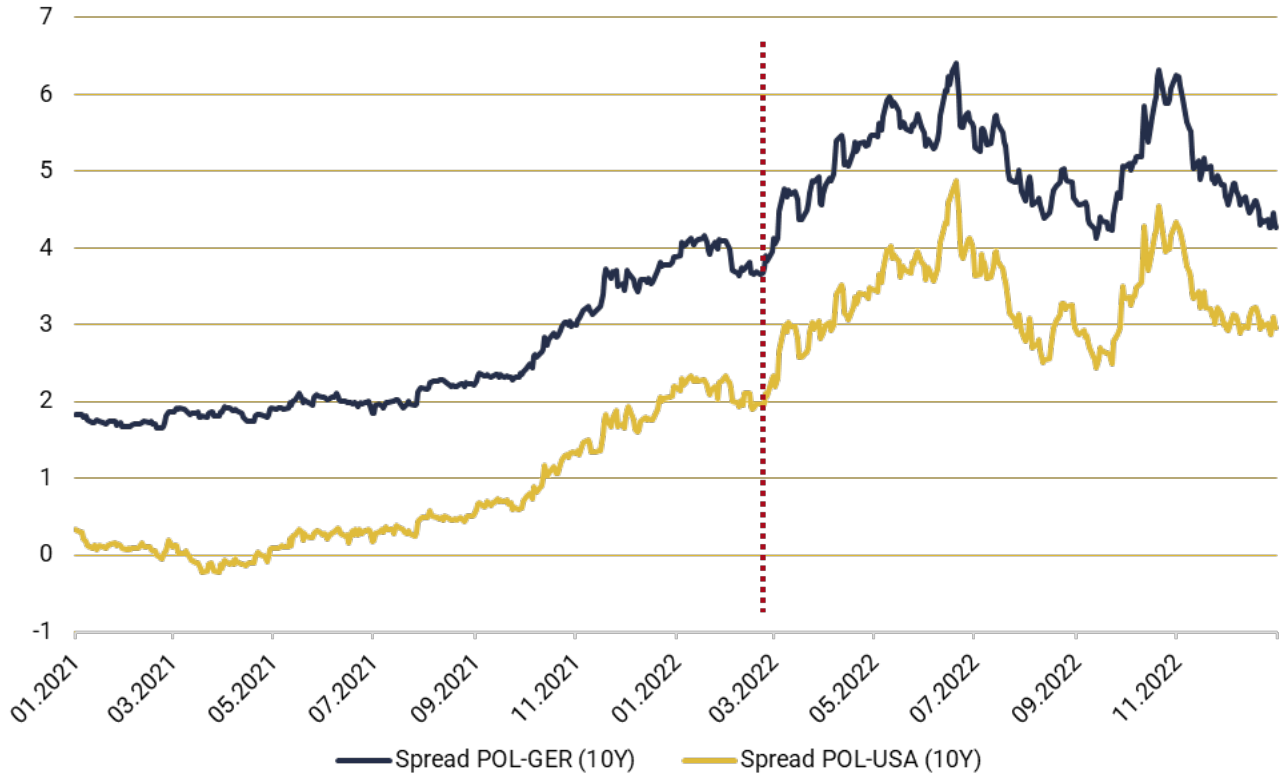
Źródło: Opracowanie własne.

Wykres 16. Rentowność 10-letnich obligacji skarbowych w latach 2021–2022 (event study)



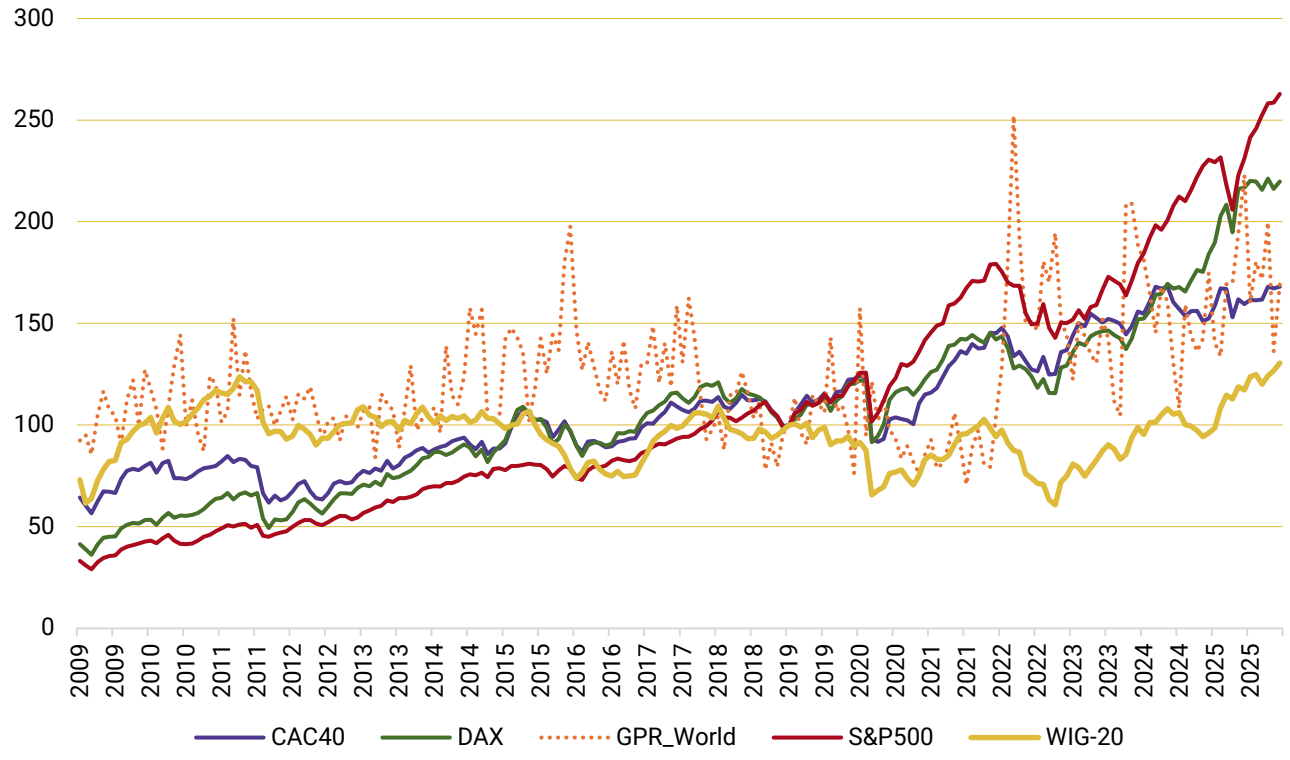
Źródło: Opracowanie własne.

Wykres 17. Różnice rentowności 10-letnich obligacji skarbowych w latach 2021–2022 (event study)



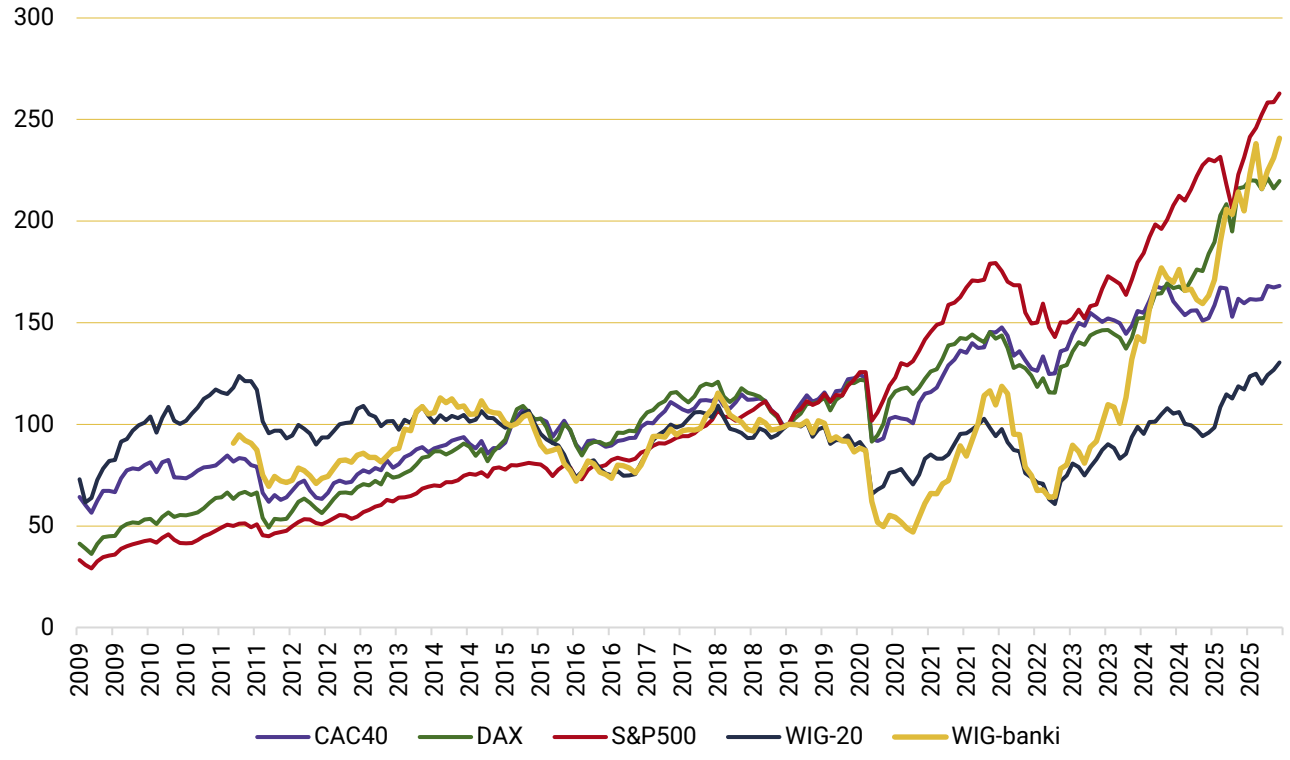
Źródło: Opracowanie własne.

Wykres 18. Wybrane indeksy giełdowe oraz indeks ryzyka geopolitycznego – ujęcie ogólne (01.2019=100)



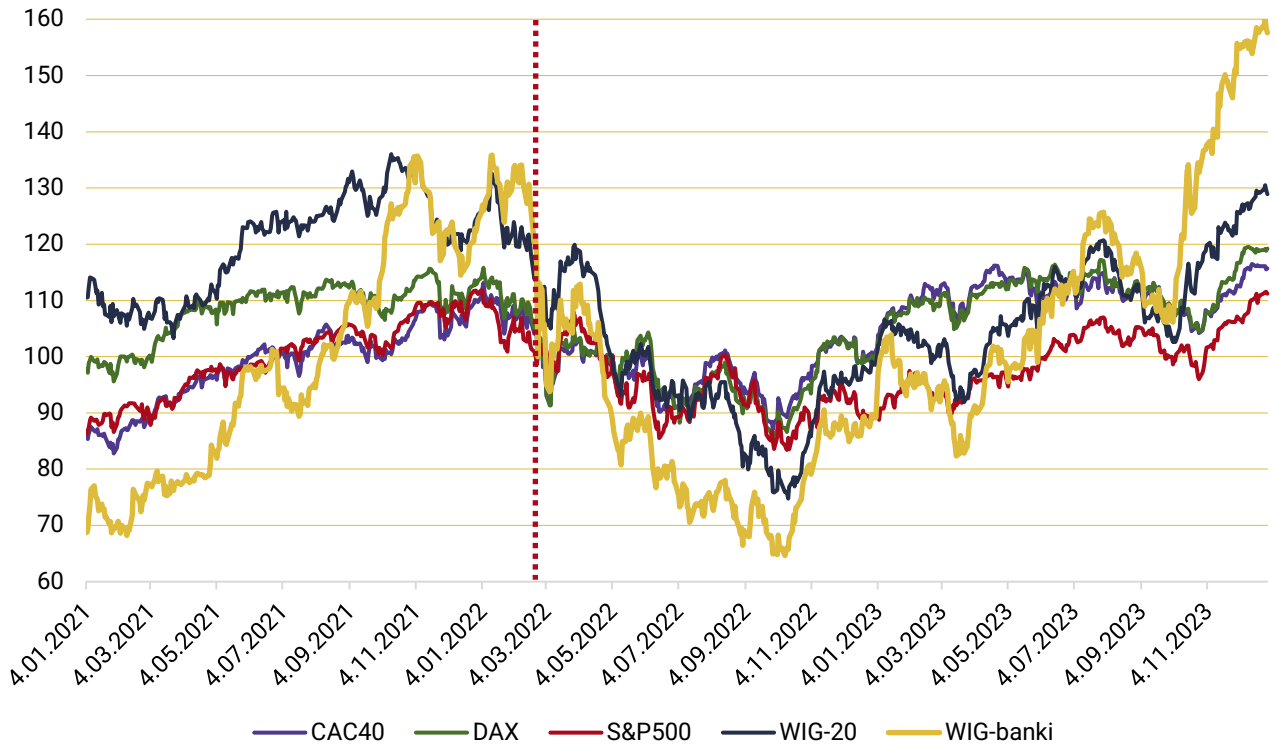
Źródło: Opracowanie własne.

Wykres 19. WIG-banki na tle wybranych indeksów giełdowych – ujęcie ogólne (01.2019=100)



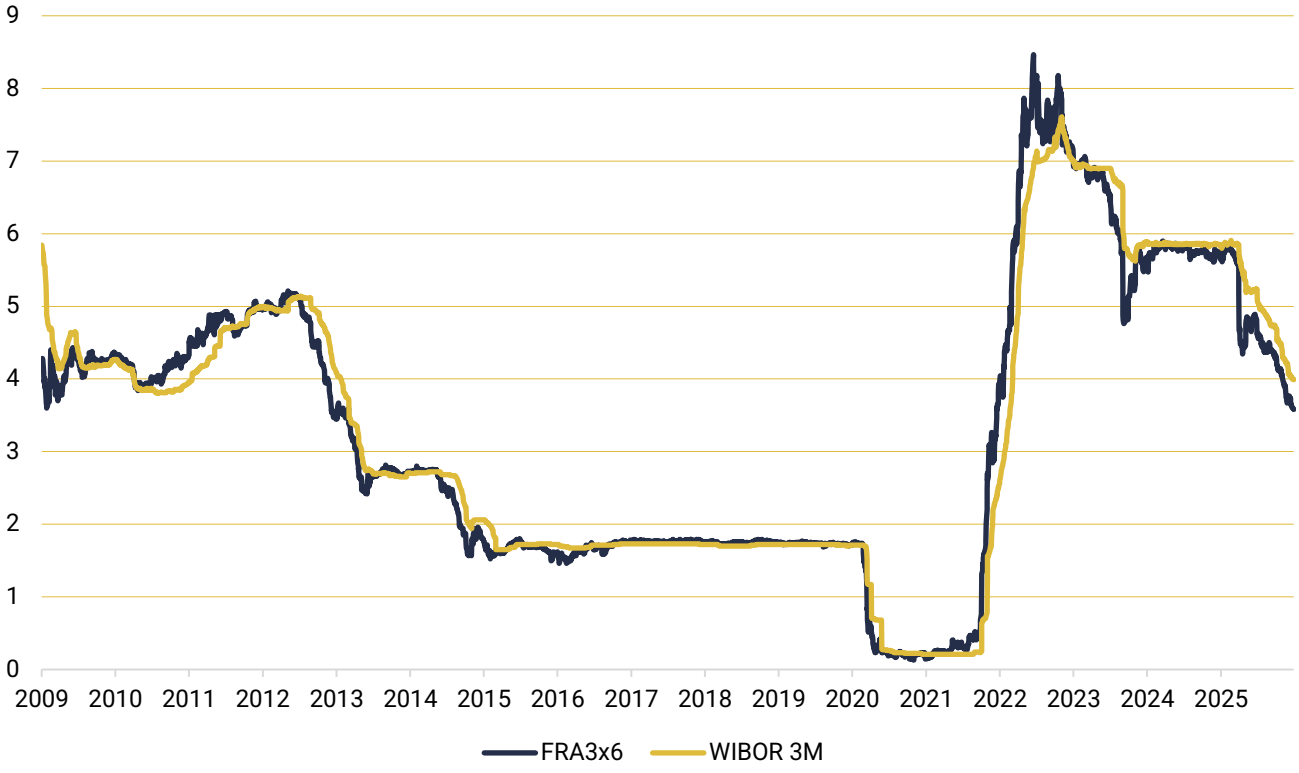
Źródło: Opracowanie własne.

Wykres 20. WIG-banki na tle wybranych indeksów giełdowych – event study (24.02.2022=100)



Źródło: Opracowanie własne.

Wykres 21. Kształtowanie się FRA3x6 oraz WIBOR 3M w latach 2009–2025

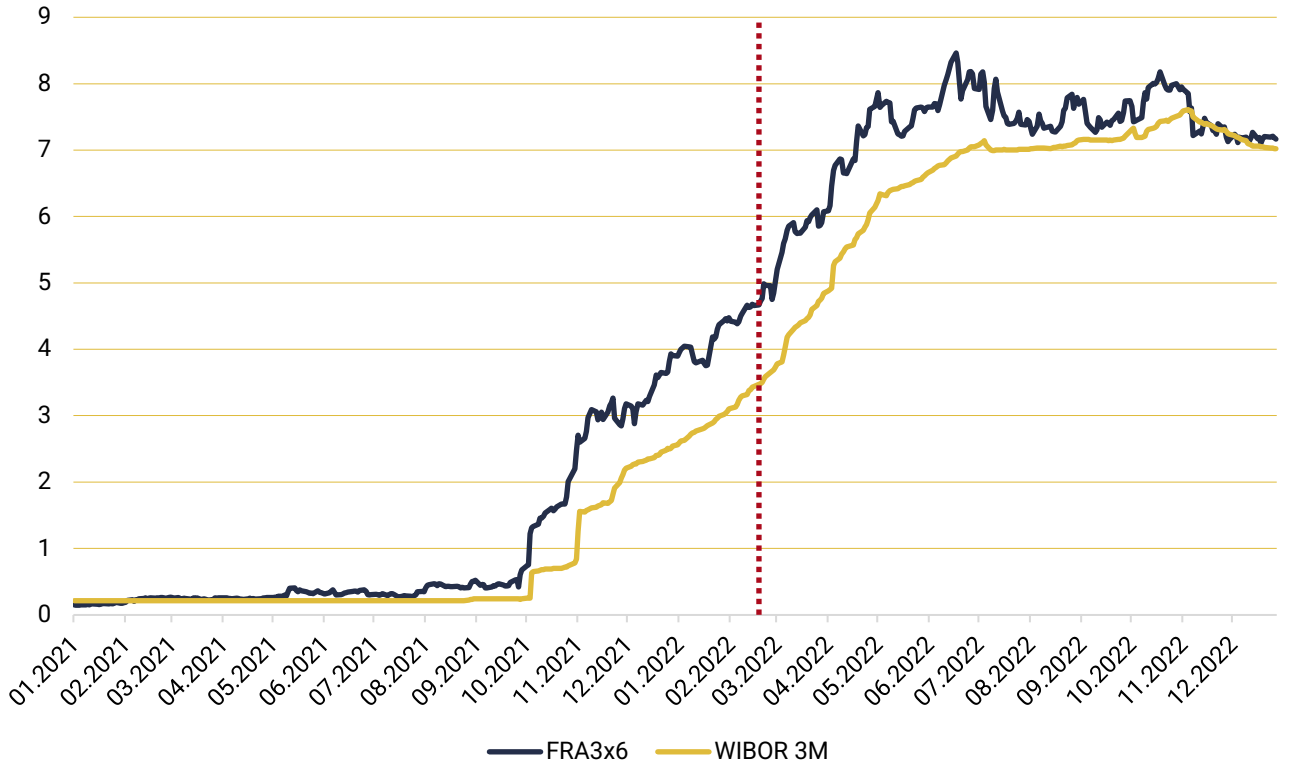


Źródło: Opracowanie własne.

Wykres 22. Różnica FRA3x6 oraz WIBOR 3M w latach 2009–2025

Źródło: Opracowanie własne.

Wykres 23. Kształtowanie się FRA3x6 oraz WIBOR 3M w latach 2021–2022 (event study)



Źródło: Opracowanie własne.

Wykres 24. Różnica FRA3x6 oraz WIBOR 3M w latach 2021–2022 (event study)

Źródło: Opracowanie własne.

W sytuacji wzrostu ryzyka geopolitycznego, w warunkach wojny hybrydowej (poniżej progu artykułu 5. NATO) można spodziewać się prób testowania odporności Polski na realizację poszczególnych rodzajów ryzyka geopolitycznego. Stąd można spodziewać się takich incydentów jak np. cyberataki na polski system bankowy, działania dezinformacyjne (kanał zaufania), czy nawet ataki na infrastrukturę krytyczną. Rodzi to konieczność wypracowania skutecznych metod i sposobów ograniczania ryzyka geopolitycznego, a także stawia przed polskimi bankami określone wyzwania. Spośród nich warto zwrócić uwagę na następujące obszary: (1) aspekty techniczne; (2) kwestie finansowania obronności; (3) kwestie finansowania energetyki oraz (4) warunki wojny hybrydowej. Zagadnienia te są przedmiotem rozważań w punkcie 4.3. Przed ich rozwinięciem należy zaznaczyć, iż kwestie te – w szerszym kontekście ryzyka geopolitycznego – wymienia się w raportach dotyczących stabilności systemu finansowego w Polsce. Przykładowo, według raportu Europejskiego Kongresu Finansowego (2025) najważniejszym czynnikiem determinującym sytuację polskiego systemu finansowego w najbliższych trzech latach będzie właśnie ryzyko geopolityczne połączone ze wzrostem zagrożeń dla cyberbezpieczeństwa. Kwestie związane z utrzymaniem braku zakłóceń w działaniu infrastruktury krytycznej, utratą danych, przerwami w świadczeniu usług i spadkiem zaufania klientów stają się kwestiami o kluczowym charakterze dla bezpiecznego funkcjonowania systemu finansowego.

4.3. Wybrane wyzwania stojące przed polskim systemem bankowym w kontekście ryzyka geopolitycznego

4.3.1. Aspekty techniczne

Polskie banki opierają swoje rozwiązania operacyjne na zróżnicowanej i rozproszonej infrastrukturze informatycznej. Często łączy ona w sobie systemy zakupione od międzynarodowych dostawców, rozwiązania oparte o chmurę obliczeniową, rozwiązania rozwijane wewnętrznie przez banki oraz moduły integracyjne łączące środowiska wewnętrzne z zasobami zewnętrznymi. Taka heterogeniczna architektura, w której stosuje się różne platformy techniczne i lokalizacje zasobów, zgodnie z koncepcją bezpie-

czeństwa przez różnorodność, hipotetycznie **może zwiększać odporność na część cyberzagrożeń**. Niższe jest bowiem ryzyko, że luka w jednym obszarze (komponencie) infrastruktury IT pojedynczego banku automatycznie przełoży się na kompromitację pozostałych banków w sektorze.

W ocenie odporności sektora bankowego na cyberataki istotny jest nie tylko aspekt infrastruktury IT, lecz także zdolność skutecznego reagowania na incydenty i odtwarzania usług bankowych. Zdolności te obejmują w szczególności procedury klasyfikacji i eskalacji incydentów, izolacji skompromitowanej infrastruktury, komunikacji kryzysowej, przełączenia na zasoby zapasowe oraz odtworzenia danych i usług z kopii zapasowych. W warunkach silnych współzależności infrastrukturalnych w sektorze bankowym o skali skutków incydentu decyduje nie tylko sama skuteczność ataku, ale również jakość i regularne testowanie planów odtwarzania i ciągłości działania.

Ważnym przykładem ćwiczenia odporności operacyjnej sektora bankowego na cyberataki były ćwiczenia Cyber-EXE Polska 2024, zorganizowane przez Fundację Bezpieczna Cyberprzestrzeń, w których uczestniczyły wybrane banki oraz CSIRT KNF, CSIRT NASK, CSIRT GOV i CSIRT MON. Ćwiczenia te objęły warstwę techniczną (CyberRange), informacyjną (CyberBastion) oraz procesową, co pozwoliło równolegle testować analizę techniczną incydentu, proces decyzyjny i współpracę instytucjonalną. Należy jednak zaznaczyć, że ćwiczenia objęły jedynie część sektora bankowego, dlatego nie pozwalają na ocenę gotowości wszystkich banków.

Wnioski wyciągnięte z przebiegu ćwiczeń pozwoliły na identyfikację słabych punktów, poprawę współpracy i sformułowanie rekomendacji dla kolejnych edycji ćwiczeń. **Po pierwsze**, pozwoliły ocenić stopień przygotowania banków do funkcjonowania w reżimie DORA, pokazując jednocześnie, że w przyszłych edycjach konieczne jest włączenie kluczowych dostawców usług zewnętrznych, aby sprawdzić skuteczność komunikacji i reakcji na incydenty związane z usługami ICT świadczonymi przez strony trzecie. **Po drugie**, choć scenariusze ćwiczeń były oparte na rzeczywistych incydentach i umożliwiły weryfikację założonych celów, okazały się zbyt uproszczone i zbyt mało zróżnicowane. W kolejnych edycjach symulacje incydentów powinny obejmować bardziej złożone przypadki, wymagające ścisłej koordynacji między zespołami technicznymi, osobami zarządzającymi incydentem, przedstawicielami biznesu i kadrą zarządzającą. **Po trzecie**, ćwiczenia potwierdziły, że współpraca między instytucjami przynosi wymierne korzyści. W warunkach pełnej współpracy odnotowano szybsze zgłoszenia incydentów oraz wyższą jakość przekazywanych informacji o wskaźnikach kompromitacji. Ukazuje to potrzebę dalszego rozwijania szkoleń, warsztatów i procedur wspierających komunikację oraz wymianę danych w czasie rzeczywistym. Po czwarte, istotnym problemem okazał się brak jednolitego podejścia do raportowania i wymiany wskaźników kompromitacji, zarówno wobec regulatora, jak i wewnątrz samych banków. Wskazane byłoby opracowanie wspólnych wytycznych dotyczących zakresu, formatu i sposobu przekazywania takich danych, co mogłoby poprawić sprawność reagowania na incydenty w skali całego sektora (Fundacja Bezpieczna Cyberprzestrzeń, 2024).

Główne funkcje systemu finansowego, w szczególności rozliczenia płatności, realizowane są w oparciu o scentralizowane systemy zewnętrzne, takie jak SORBNET3, TARGET-NBP, Elixir czy BLIK. W takim modelu centralne komponenty rozliczeniowe i autoryzacyjne odgrywają kluczową rolę w dostarczaniu usług płatniczych i łączności między bankami. Jednocześnie ich pozycja w architekturze oznacza, że ich dostępność i integralność są krytyczne dla funkcjonowania całego systemu finansowego. W scenariuszu skrajnym, zakładając jednoczesne poważne problemy z realizacją planów odtwarzania po awarii, po skutecznym cyberataku na operatora centralnych systemów rozliczeniowych mogłoby dojść do czasowej, szerokiej niedostępności podstawowych usług rozliczeniowych i płatniczych. Taki stan mógłby doprowadzić do paraliżu przelewów międzybankowych, opóźnień w płatnościach oraz wywołać spadek zaufania klientów, a w konsekwencji potencjalnie do paniki i chaosu informacyjnego w warunkach poważnego kryzysu cybernetycznego. W zależności od skali i czasu trwania zakłóceń, możliwe byłyby też efekty drugoplanowe, takie jak presje płynnościowe dla instytucji finansowych, negatywny wpływ na rynki finansowe oraz obciążenie organów nadzorczych i systemu publicznego reagowania kryzysowego.

Nawet jeśli poszczególne banki komercyjne skrupulatnie wdrażają wymogi odporności cyfrowej (DORA), sektor bankowy nadal funkcjonuje jak zestaw naczyń połączonych. W scenariuszu skrajnym udany cyberatak na jeden z kluczowych podmiotów, zwłaszcza operatorów centralnych systemów rozliczeniowych, może spowodować szerokie zakłócenia w funkcjonowaniu całego sektora. Skutki takich zdarzeń obejmują niedostępność usług płatniczych, paraliż operacji bankowych, panikę wśród klientów oraz destabilizację zaufania do systemu finansowego, generując efekt domina, który rozciąga się od infrastruktury technicznej po społeczny odbiór sektora.

Spośród centralnych systemów rozliczeniowych istotnych dla polskiego sektora bankowego szczególnie wysoką odpornością operacyjną wyróżnia się europejski system TARGET, służący do rozrachunku płatności w euro. Jego odporność wynika z rozproszenia infrastruktury między dwa regiony i cztery ośrodki przetwarzania danych, a także z jasno określonych i regularnie testowanych procedur awaryjnych. W efekcie nawet poważna awaria jednego z kluczowych elementów systemu nie musi prowadzić do wstrzymania rozrachunku płatności w euro, ponieważ obsługa może zostać przejęta przez inny ośrodek lub objęta rozwiązaniami zapasowymi dla płatności krytycznych (ECB, 2026). W odniesieniu do rozrachunku płatności w polskim złotym zasadne byłoby dalsze wzmacnianie istniejących mechanizmów awaryjnych poprzez wykorzystanie dobrych praktyk stosowanych w systemie TARGET, tak aby w razie poważnego incydentu operacyjnego lub cyberataku możliwe było utrzymanie lub szybkie przywrócenie realizacji krytycznych rozrachunków.

4.3.2. Rola sektora w finansowaniu obronności

W obliczu wzrostu (wskutek opisanych wcześniej zjawisk i procesów) ryzyka geopolitycznego w krajach UE (w tym i Polsce), Komisja Europejska i rządy poszczególnych krajów podjęły decyzje o znaczącym zwiększeniu wydatków na obronność. Po wybuchu wojny w Ukrainie w 2022 r., od 2023 r. wydatki na obronność w krajach UE sukcesywnie wzrastały. W 2025 r. największe wydatki w relacji do PKB miały Estonia (3,37% w porównaniu do 2,14% w 2022 r.) i właśnie Polska (4,5% w porównaniu do 2,20% w 2022 r.) (Zob. tabela 5). Jednak przy zwiększonym GPR coraz częściej pojawiają się opinie, że taki poziom finansowania obronności jest niewystarczający i powinno to być minimum 3% PKB. W grudniu 2025 r. NATO zarekomendowało dalszy wzrost wydatków rządowych na obronność do poziomu 5% PKB do 2035 r. (NATO, 2025).

Charakterystyczne jest, że wzrost wydatków na obronność był zróżnicowany geograficznie. Występują również duże różnice między poszczególnymi krajami. Wydatki na obronność w latach 2000–2025 w ujęciu regionów ujęto na wykresie 25., natomiast na wykresie 26. przedstawiono strukturę tych wydatków w odniesieniu do 15 państw cechujących się najwyższymi wydatkami na obronność (w tym Polski).

Tabela 5. Udział wydatków na obronność w % PKB w okresie 2020–2025

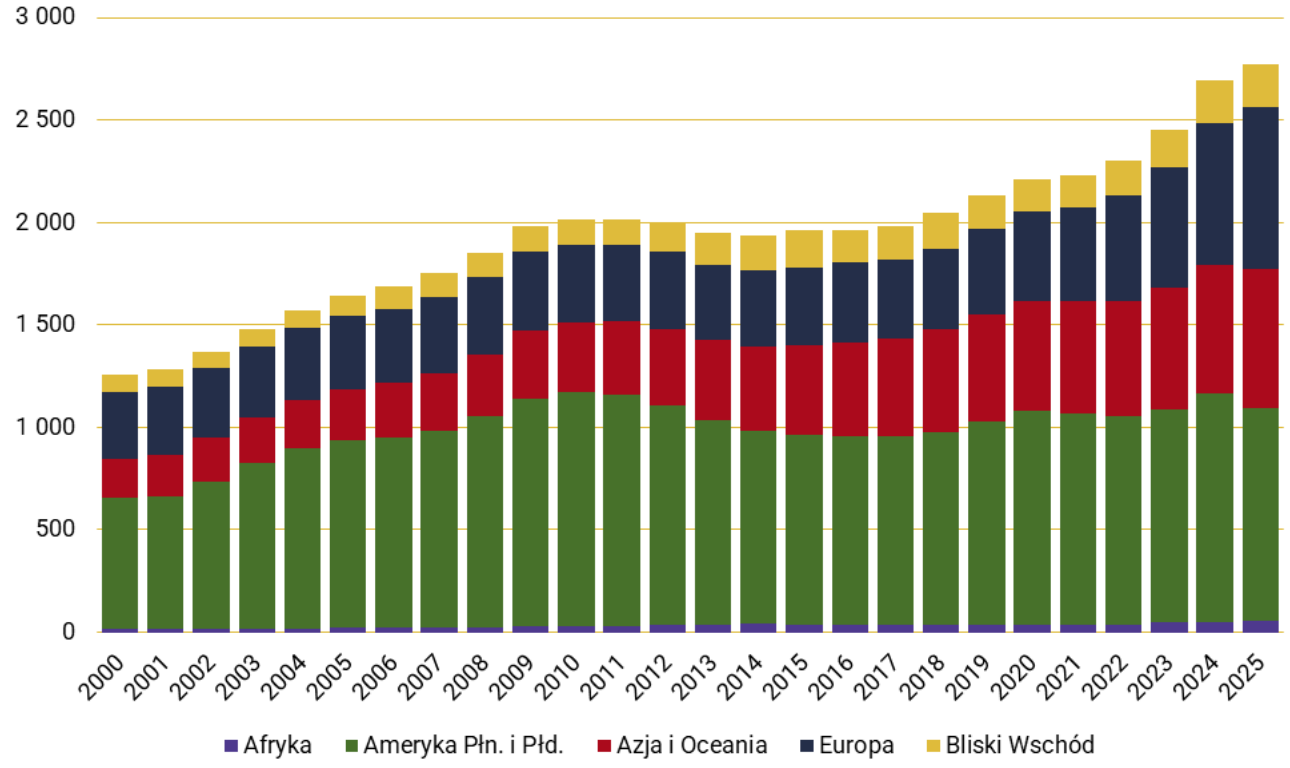
Państwo	2020	2021	2022	2023	2024	2025
Austria	**0,89**	**0,87**	**0,76**	**0,86**	**0,99**	**1,10**
Belgia	1,01	1,04	1,17	1,17	1,28	2,01
Bułgaria	1,59	1,51	1,59	1,95	1,93	2,01
Chorwacja	1,70	1,97	1,80	1,65	1,86	2,02
Cypr	1,90	1,78	1,71	1,59	1,58	1,61
Czechy	1,27	1,35	1,29	1,31	1,88	1,84
Dania	1,37	1,30	1,37	2,01	2,27	3,25
Estonia	2,26	2,01	2,14	2,98	3,30	3,37
Finlandia	1,44	1,30	1,59	2,01	2,18	2,57
Francja	2,02	1,98	1,96	1,95	2,01	2,03
Grecja	3,02	3,80	4,02	2,89	2,88	2,99
Hiszpania	1,36	1,37	1,43	1,53	1,46	2,13
Irlandia	0,26	0,24	0,21	0,22	0,22	0,22
Kanada	1,42	1,22	1,14	1,31	1,35	1,63
Litwa	2,05	1,95	2,56	2,84	3,14	3,08
Luksemburg (szacunki SIPRI)	0,49	0,41	0,57	0,68	0,66	0,85

Źródło: *SIPRI, https://www.sipri.org/databases/milex.*

Państwo	2020	2021	2022	2023	2024	2025
Łotwa	2,23	2,16	2,25	2,93	3,30	3,61
Malta	0,53	0,45	0,42	0,38	0,37	0,45
Niderlandy	1,41	1,37	1,30	1,44	1,94	2,19
Niemcy	1,36	1,30	1,34	1,50	1,84	2,27
Norwegia	1,97	1,68	1,46	1,82	2,23	3,28
Polska	**2,26**	**2,22**	**2,20**	**3,26**	**3,75**	**4,50**
Portugalia	1,44	1,52	1,36	1,21	1,44	1,71
Rumunia	2,02	1,86	1,76	1,62	2,17	2,28
Słowacja	1,83	1,65	1,78	1,74	1,98	2,03
Słowenia	1,08	1,24	1,30	1,31	1,34	1,54
Szwajcaria	0,77	0,67	0,68	0,71	0,70	0,76
Szwecja	1,15	1,20	1,34	1,52	1,99	2,47
Turcja	2,16	1,81	1,62	1,69	1,84	1,91
USA	3,64	3,40	3,30	3,29	3,43	3,12
Węgry	1,75	1,32	1,84	2,04	2,12	2,04
Wielka Brytania	2,14	2,04	2,01	2,15	2,44	2,35
Włochy	1,66	1,61	1,60	1,53	1,59	1,89

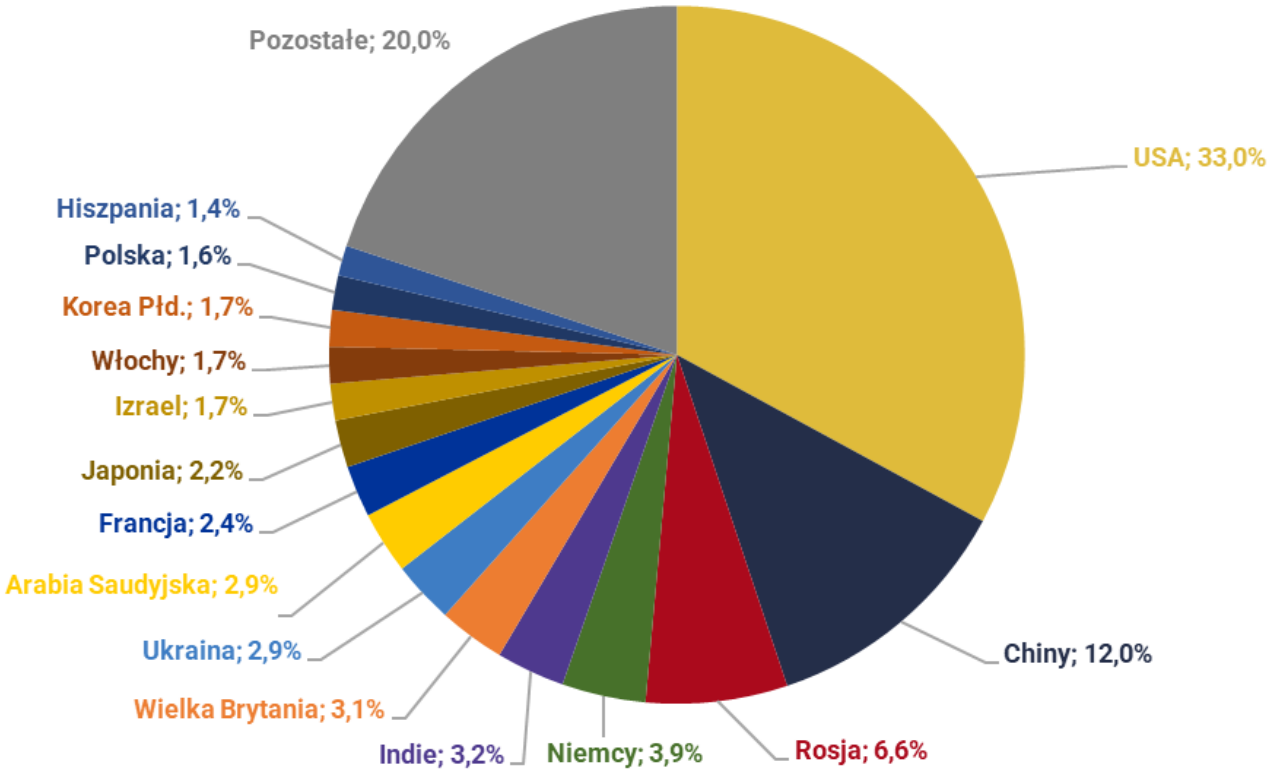
Źródło: *SIPRI, https://www.sipri.org/databases/milex.*

Wykres 25. Wydatki na obronność w latach 2000–2025 wg regionów (w stałych USD z 2024r., w mld)



Źródło: Opracowanie własne na podstawie: SIPRI (2026).

Wykres 26. Struktura wydatków na obronność – 15 krajów o największych wydatkach w tym zakresie



Źródło: Opracowanie własne na podstawie: SIPRI (2026).

W 2025 r. nominalnie największe wydatki z grupy państw NATO miały USA (3,1% PKB; 954 mld USD; udział 33% w ogółem wydatkach na świecie), Niemcy (2,3% PKB; 114 mld USD; 3,9%), Wielka Brytania (2,4%; 89,0 mld USD; 3,1%)[66]. Wśród krajów NATO, to USA wydają najwięcej. Według danych SIPRI światowe wydatki militarne wzrosły o 2,9% w porównaniu z rokiem poprzednim, do rekordowego poziomu 2887 mld USD. Był to przy tym jedenasty kolejny rok wzrostu tych wydatków (SIPRI, 2026).

Zwiększenie wydatków na obronę na świecie, w tym w krajach UE, stało się zatem faktem. W Polsce tendencja wzrostowa wydatków na obronność jest widoczna od 2022 roku, kiedy to ze względu na wojnę w Ukrainie Polska zwiększyła inwestycje w zbrojenia i bezpieczeństwo narodowe. Uchwalona w 2022 r. Ustawa o obronie Ojczyzny zakłada minimalny poziom wydatków obronnych na poziomie co najmniej 3% PKB, przy założeniu, że co najmniej 20% z tych środków zostanie przeznaczonych na wydatki majątkowe (tzn. związane głównie z zakupami sprzętu wojskowego). Według danych GUS, w Polsce – wydatki na obronność wyniosły w 2024 r. 134 mld zł, co stanowiło niecałe 4% PKB (stanowi to sumę budżetu MON i Funduszu Wsparcia Sił Zbrojnych, obsługiwanego przez BGK)[67]. W ustawie budżetowej na rok 2025, łączne zaplanowane wydatki obronne wyniosły 187 mld zł, z czego 124,3 mld zł w ramach budżetu państwa, a pozostała część z Funduszu Wsparcia Sił Zbrojnych – łącznie 4,7% PKB. Natomiast w ustawie budżetowej na 2026 r. wydatki na obronę są planowane na poziomie 200 mld PLN, tj. 4,8% PKB.

Wydatki na obronność są zasadniczo finansowane z budżetów państw, bo obrona narodowa jest obowiązkiem państwa. Mają one przy tym różny charakter; wśród nich najważniejszymi kategoriami są: ochrona ludności (np. budowa schronów), obrona cywilna, usługi na potrzeby bieżącego utrzymania sił zbrojnych, uposażenie żołnierzy, oraz inwestycje i zakup sprzętu wojskowego. Ta ostatnia kategoria wiąże się z wydatkami na techniczną modernizację i utrzymanie sprawności operacyjnej armii. Decyzje o tych wydatkach mają dalekosiężne skutki dla budżetu państwa, wzrostu gospodarczego, rozwoju krajowego przemysłu zbrojeniowego, a także dla **instytucji finansowych** obsługujących przedsiębiorstwa z tego sektora. Skutki te wynikają (są konsekwencją) z kilku kwestii.

66 Dla porównania, w tym roku wydatki obronne Rosji wynosiły 7,1% PKB (149 mld USD; 5,5% w wydatkach ogółem na świecie), Chin – 1,7% PKB (314 mld USD, 12%), a Ukrainy – 34% PKB (64,7 mld USD; 2,4%) (SIPRI, 2025).

67 Różnice między wysokościami wydatków prezentowanymi przez Eurostat i polski rząd wynikają z tego, że uwzględnione są wydatki na obronność wydatkowane przez FWSZ, zarządzany przez BGK – nie są one ujmowane jako deficyt budżetowy.

Po pierwsze, **wydatki na zakup sprzętu w danym roku oznaczają wzrost wydatków na jego obsługę i utrzymanie**, co generuje dodatkowe wydatki w następnych latach (dekadach), które muszą być sfinansowane. Pojawia się pytanie nie tylko o możliwość i sposoby sfinansowania samych inwestycji, ale i o utrzymanie tego sprzętu w gotowości operacyjnej. Szacuje się, że nowy sprzęt powinien być utrzymywany w gotowości i sprawności przez kolejne co najmniej 30–40 lat, co jest kosztowne. Koszty cyklu życia sprzętu zbrojeniowego są około dwóch do trzech razy wyższe niż kwota zakupu i dlatego mogą mieć znaczący wpływ na roczne wydatki budżetowe (Department of Defence, 2026).

Po drugie, **ważne jest, od kogo nabywany jest ten sprzęt**: z kraju („local content") czy z zagranicy. Pierwszy przypadek jest najkorzystniejszy dla gospodarki, gdyż pojawiają się efekty mnożnikowe inwestycji (wzrost transakcji i płaconych podatków przez uczestników łańcucha dostaw, wzrost możliwości wydatkowania na obronę z budżetu państwa), wzrasta dynamika PKB, zwiększa się krajowy potencjał produkcyjny sektora obronnego, możliwy jest eksport. Jeśli te wydatki ponosi się na produkty importowane, to jest mniej pozytywnych skutków (zawsze jednak jest to zwiększenie bezpieczeństwa narodowego). Dlatego w takim przypadku ważne jest podpisanie odpowiednich korzystnych kontraktów wiążących zakup z transferem technologii, know-how. Sprzęt taki też powinien być nabywany z krajów członkowskich NATO czy UE lub krajów, które są zweryfikowane przez NATO (np. Korea Płd.).

W tym miejscu warto podkreślić, iż taki model przyjęto w Polsce. Wśród głównych dostawców sprzętu są obecnie: **1. Stany Zjednoczone** (myśliwce wielozadaniowe F-35A oraz F-16, czołgi Abrams, systemy obrony powietrznej Patriot, systemy artylerii rakietowej HIMARS., śmigłowce szturmowe AH-64E Apache; **2. Korea Południowa** (czołgi: K2 Black Panther (i planowana wersja K2PL), armatohaubice: K9A1 Thunder, lekkie samoloty bojowe FA-50, wyrzutnie rakiet: K239 Chunmoo (odpowiednik HIMARS); **3. Polski przemysł obronny – Polska Grupa Zbrojeniowa (PGZ)** (m.in. armatohaubice Krab, kołowe transportery opancerzone Rosomak (na fińskiej licencji), broń strzelecka: Karabinki MSBS Grot, produkowane przez Fabrykę Broni „Łucznik" w Radomiu; przenośne zestawy rakietowe Piorun, systemy Poprad, zestawy Pilica i Pilica+).

Ponadto, innymi dostawcami są m.in. **Szwecja** (samoloty wczesnego ostrzegania Saab 340 AEW, a w przeszłości m.in. wyrzutnie przeciwlotnicze), **Izrael** (radary brzegowe i inne elementy systemów elektronicznych) oraz **Turcja** (drony Bayraktar TB2). Kierunek europejski oraz krajowy zakłada się również w odniesieniu do zakupów finansowanych z programu SAFE.

Po trzecie, zwiększone zakupy sprzętu wojskowego przyczyniają się do zwiększenia inwestycji w przemysł zbrojeniowy i jego potencjału produkcyjnego w kraju. Przedsiębiorstwa z sektora zbrojeniowego mogą być własnością prywatną (większość przedsiębiorstw z tego sektora w USA, Wielkiej Brytanii) lub państwową (np. w Polsce – PGZ). Najwięksi producenci na świecie to zarówno przedsiębiorstwa prywatne (np. Lockheed Martin z USA, BAE Systems z W. Brytanii, Boeing z USA, Elbit Systems z Izraela, Leonardo z Włoch, Rheinmetall z Niemiec, Dassault Aviation z Francji, Czechoslovak Group z Czech), jak i państwowe (Rostec z Rosji, AVIC z Chin, Thales z Francji (udział SP 26,6%), Israel Aerospace Industries z Izraela, ASELSAN z Turcji, PGZ z Polski)[68].

Po czwarte wreszcie, dobrze jeśli są to inwestycje w produkcję produktów podwójnego zastosowania tzw. *dual use*, obejmujące towary, oprogramowanie i technologie, które można wykorzystywać zarówno w celach cywilnych, jak i wojskowych.

Z tych względów dobór źródeł finansowania i zapewnienie odpowiedniej obsługi strumieni pieniężnych wynikających z tego typu inwestycji stają się sprawą absolutnie kluczową. W państwach członkowskich UE planowane zwiększone wydatki na obronę przez państwa mogą być finansowane z następujących źródeł: (1) programu Komisji Europejskiej – Plan *ReArm Europe*; (2) zwiększonych wydatków na obronę finansowanych z zaciągniętego długu publicznego, zwiększonych podatków, wprowadzenia specjalnego podatku; (3) KPO oraz (4) kredytów lub pożyczek z banków komercyjnych.

Rolę dla instytucji bankowych przewidziano w uruchomieniu każdego z tych źródeł, jednak z punktu widzenia celu raportu, szczególną uwagę warto zwrócić na ten ostatni punkt, w którym banki występują *explicite*. Niewątpliwie, planowane wydatki KE i poszczególnych rządów UE wskazują, że sektor zbrojeniowy jest aktualnie (2025–2026) traktowany priorytetowo przez te instytucje. Wysoki popyt na produkty tego sektora ze strony oficjalnych podmiotów kreuje wysokie potrzeby inwestycyjne, a finansowanie rozwoju potencjału zbrojeniowego i jego dalsza obsługa mogą być zyskowne i bezpieczne. Zapowiadany

68 Wszystkie wymienione przedsiębiorstwa należały w 2024 r. do 51 największych na świecie (według przychodów). (https://www.sipri.org/sites/default/files/2025-11/fs_2512_top_100_2024.pdf, dostęp 22.01.2026).

rozwój przemysłu obronnego w Europie może być dla banków okazją do zawierania korzystnych umów kredytowych. Wydatki na obronność finansuje państwo, a banki mogą (współ)finansować zarówno rozwój mocy produkcyjnych, jak i produkcję uzbrojenia. W oczywisty sposób, skorzystają na tym wszystkie zaangażowane podmioty, a ostatecznym rezultatem (oprócz tendencji prowzrostowych) będzie obniżenie ryzyka geopolitycznego poprzez zbudowanie odpowiedniej siły odstraszania.

By jednak banki mogły aktywnie partycypować w rozbudowie potencjału obronnego i wykorzystać wiążące się z tym szanse, konieczne jest rozwiązanie kilku problemów natury systemowej. Mianowicie, w odniesieniu do udzielania kredytów dla przedsiębiorstw zbrojeniowych (albo, na bardziej ogólnym poziomie, bezpośredniego i pośredniego zaangażowania kapitałowego w tego typu podmiotach) oraz obsługi przez banki przepływów pieniężnych wiążących się z wydatkami na obronność, w krajach UE, a w tym i w Polsce, pojawiają się pewne istotne bariery.

Po pierwsze, sektor bankowy jest, z samej swojej natury i charakteru banków jako instytucji zaufania publicznego, najbardziej regulowanym sektorem w gospodarce. W kontekście udziału finansowania przemysłu zbrojeniowego należy tu zwłaszcza wziąć pod uwagę następujące kwestie:

1. **Limity zaangażowania** – względy stabilności systemowej nakazują utrzymywanie ograniczeń koncentracji zaangażowania kapitałowego banku w pojedyncze programy/przedsiębiorstwa. W warunkach polskich, zgodnie z prawem bankowym oraz rozporządzeniem CRR, bank nie może zasadniczo przyjąć ekspozycji (kredyty, gwarancje) wobec pojedynczego klienta lub grupy powiązanych klientów, która przekracza 25% wartości kapitału Tier 1 banku.
2. Stąd, utrudnione bądź nawet wykluczone przy danym stanie prawnym może być sfinansowanie dużych projektów przekraczających prawne limity zaangażowania banku w dane przedsięwzięcie – a projekty inwestycyjne w sektorze zbrojeniowym (ale także w zakresie inwestycji w infrastrukturę oraz, energetykę) są kosztowne i długoterminowe. Pewnym wyjściem jest tu utworzenie konsorcjum przez banki i zawieranie długoletnich umów na finansowanie, ale i to może nie wystarczyć.
3. **Ekspozycja na ryzyko kredytowe**: inwestycje w sektorze zbrojeniowym są długoterminowe, sprzedaż produktów może pojawić się dopiero po latach i w związku z tym spłaty kredytów będą odroczone. Dlatego też ważne jest zapewnienie przez rząd (głównego odbiorcę sprzętu) długoterminowości zamówień, co skłoni krajowych przedsiębiorców do inwestycji i zaciągania kredytów oraz zwiększy ich wiarygodność kredytową. Dotyczy to całego sektora, ale w szczególności finansowania inwestycji start-upów, projektujących zaawansowany technologicznie, innowacyjny sprzęt i technologie, co jest obarczone wysokim ryzykiem.
4. **Relacja transparentność umów – dostęp do informacji niejawnych** w sektorze zbrojeniowym: kontrakty w sektorze zbrojeniowym są podporządkowane bardzo rygorystycznym procedurom ze względu na bezpieczeństwo kraju i kontrolę technologii przez przedsiębiorstwa i państwo. Dlatego przy dostępie do informacji niejawnych konieczne są specjalne procedury i zachowanie poufności. Banki natomiast są pod nadzorem organów regulacyjnych, które wymagają ujawniania (*disclosure*) informacji, a w przypadku takich kontraktów nie jest to możliwe (i raczej nie powinno być).

Po drugie, banki powinny działać zgodnie z kryteriami ESG (ang. *Environmental, Social and Governance*) i zasadami finansowania zrównoważonego. W krajach UE obowiązują dość restrykcyjne ramy zrównoważonego inwestowania (*sustainable investment framework*), oparte na kryteriach ESG. Zgodnie z nimi, z uwagi na względy prawne, etyczne i reputacyjne, branża obronności jest uznawana za tzw. „grzeszne spółki" (ang. *sin stock*). Status taki przez lata był uznawany przez banki za jedną z głównych barier inwestycji w niektóre rodzaje uzbrojenia. Efekt ten jest przy tym wzmacniany przez kwestie reputacyjne ze strony banków (tego typu inwestowanie może być negatywnie postrzegane przez interesariuszy banków), dla których dodatkowym czynnikiem jest tu raportowanie wewnętrzne, mające na celu zarządzanie kwestiami zrównoważonego rozwoju i ocenę portfela w tym aspekcie.

W obliczu zwiększonego RGP pojawiają się głosy o konieczności rozluźnienia kryteriów ESG, tym bardziej, że te ograniczenia nie dotyczą instytucji finansowych spoza UE (a więc np. z USA, Chin i Rosji, które są liderami w rozwoju sektora obronnego). Wśród rozważanych i już podejmowanych działań w zakresie rozluźnienia zasad ESG w stosunku do sektora zbrojeniowego można wskazać następujące:

1. W raporcie NATO *Innovation Fund*[69] pt. „Odpowiedzialne inwestowanie w obronę, bezpieczeństwo i odporność" (luty 2025 r.) wskazano, że wyklu-

69 Innovation Fund to fundusz typu venture capital, wspierany przez 24 państwa należące do NATO, który inwestuje ponad 1 miliard euro w innowacje obronne.

czenie przedsiębiorstw z sektora obronnego z zakresu finansowania ich działalności przez instytucje finansowe (banki, fundusze emerytalne, fundusze inwestycyjne) jest jedną z głównych barier wzrostu wydatków na obronność w Europie. Przyczyną tego jest stosowanie kryteriów ESG i regulacje wewnętrzne instytucji finansowych, co odcina przedsiębiorstwa z tego sektora od pożyczek, kapitału, ubezpieczeń. Ma to negatywny wpływ na zdolności produkcyjne przedsiębiorstw z sektora obronnego, ich inwestycje i innowacje. Jak napisano: „Branża, która chroni europejskie demokracje i wartości, nie powinna być klasyfikowana jako nieetyczna i wykluczona". Stąd postulat, aby **zasady ESG w sektorze finansowym zostały uzupełnione o cele obronne**.

2. EBI wskazuje na możliwości długoterminowe finansowania przemysłu zbrojeniowego, co stanowi już pewną wskazówkę dla innych banków w krajach UE.

3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2464 z dnia 14 grudnia 2022 r. (znana jako Corporate Sustainability Reporting Directive, CSRD) wprowadziła obowiązek raportowania zrównoważonego rozwoju – ESG (ang. *Environmental, Social and Governance*) – dla wszystkich dużych jednostek oraz małych i średnich spółek giełdowych. Dyrektywa CSRD została wdrożona w Polsce ustawą z dnia 6 grudnia 2024 r. o zmianie ustawy o rachunkowości, ustawy o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym oraz niektórych innych ustaw (Dz.U. 2024 poz. 1863). Dnia 16 kwietnia 2025 r. opublikowano Dyrektywę Parlamentu Europejskiego i Rady (UE) 2025/794, tzw. *stop-the-clock*, która przewiduje dwuletnie odroczenie terminu raportowania w zakresie zrównoważonego rozwoju dla spółek, które miały rozpocząć raportowanie po raz pierwszy za rok obrotowy 2025 lub 2026 (sporządzą one pierwsze raporty dopiero odpowiednio za lata 2027 i 2028).

Wyraźną tendencją w UE jest zmiana postrzegania natury sektora zbrojeniowego, który ponownie jest uznawany za dobro publiczne w czasach wzrastającego RGP, o czym świadczy program ReArm. Rządy w krajach UE widzą potrzebę współpracy z sektorem bankowym w celu wsparcia finansowego rozwoju sektora obronnego. Jako przykłady można podać: we Francji ministerstwo finansów zorganizowało konferencję w marcu 2025, która zgromadziła przedstawicieli rządu, sektora bankowego i przemysłu zbrojeniowego w celu zachęcenia instytucji finansowych do zwiększenia wsparcia dla francuskiej bazy industrialno-technologicznej; w Wielkiej Brytanii ponad 100 parlamentarzystów Partii Pracy podpisało list otwarty wzywający banki i fundusze inwestycyjne do złagodzenia zasad dotyczących finansowania sektora obronnego; w Polsce, Minister Finansów i Gospodarki zorganizował spotkanie przedstawicieli EBI, BGK, banków komercyjnych i przedsiębiorstw sektora zbrojeniowego (prywatnych i państwowych).

Można jednocześnie wskazać liczne już przykłady zaangażowania banków z UE, w tym z Polski, w finansowanie sektora zbrojeniowego w swoich krajach:

1. W zakresie zaangażowania w finansowanie sektora zbrojeniowego w swoich krajach prym wiodą banki francuskie: BNP Paribas, Crédit Agricole, Société Générale, BPCE, Crédit Mutuel i Banque Postale.

2. W 2017 r. francuski fundusz państwowy Bpifrance stworzył fundusz Definvest, który finansuje francuskie MŚP w sektorze obronnym, we współpracy z francuskim ministerstwem sił zbrojnych[70].

3. Banki powołują specjalne departamenty zajmujące się współpracą z sektorem zbrojeniowym.

4. Pod koniec 2025 r. PKO BP i BGK podpisały osobne porozumienia o współpracy z PGZ (PKO BP i PGZ podpisały umowę o współpracy strategicznej, podnosząc limit finansowania z 2 mld zł do poziomu 12 mld zł, głównie na budowę i rozbudowę nowych mocy produkcyjnych). Wsparcie BGK dla Grupy Kapitałowej PGZ (w grupie kapitałowej jest 69 podmiotów) dotyczy w szczególności finansowania kontraktów zbrojeniowych, projektów eksportowych, a także inwestycji.

5. Banki w Polsce są też zaangażowane pośrednio – poprzez finansowanie projektów typu *dual-use*, tj. inwestycji o charakterze infrastrukturalnym (energetyka, transport), przemysłowym i technologicznym. Wśród nich są: PKO Bank Polski, ING Bank Śląski, mBank.

6. W Polsce Fundusz Vinci, zarządzany przez BGK, zainwestował w polską firmę SR Robotics, produkującą drony podwodnego zastosowania (jest to rozwiązanie *dual use*).

Po trzecie, obowiązujące przepisy prawa antymonopolowego, fuzji i przejęć i pomocy publicznej w UE nie uwzględniają specyfiki sektora obronnego w nadzwyczajnej sytuacji wzrostu ryzyka geopolitycznego.

70 https://www.bpifrance.com/products/definvest/

KE podjęła inicjatywę w tym zakresie, przyjmując Pakiet Gotowości Obronnej (*Defence Readiness Omnibus*)[71], którego celem jest zredukowanie obciążeń regulacyjnych sektora obronnego. Jego priorytetem jest zapewnienie przejrzystości regulacyjnej oraz poczucia pewności wśród inwestorów i instytucji finansowych oraz odpowiednie dostosowanie istniejących regulacji do nowej sytuacji geopolitycznej. W dokumencie KE wskazuje się na konieczność stworzenia jednolitego europejskiego rynku obronnego. Wymaga to jednak reform na szczeblu UE oraz gotowości na szczeblu krajowym do działania w wymiarze europejskim, co rodzi wiele problemów, które KE będzie starała się rozwiązać. Są to następujące kwestie: w ramach egzekwowania prawa antymonopolowego KE zobowiązuje się w szczególności do uwzględnienia „specyfiki przemysłu obronnego", a także ambicji obronnych UE i zmienionego porządku bezpieczeństwa. W zakresie pomocy państwa, chociaż sądy UE rozważały stosowanie „wyłączenia obronnego" na mocy art. 346 TFUE, niewiele jest wytycznych poza tym. W zakresie kontroli fuzji nie jest jasne, jak należy równoważyć kwestie obronności z wpływem na konkurencję.

Osobnym aspektem jest wielkość sektora bankowego w Polsce i jego możliwości finansowania, obiektywnie niewielkie w porównaniu z sektorami Francji czy Niemiec. Niemniej, w obliczu zwiększającego się GPR, banki powinny zaangażować się w finansowanie rozwoju sektora zbrojeniowego, ale na takich zasadach, **aby – przy oczekiwanej stopie zwrotu – minimalizować ryzyko regulacyjne**, kredytowe i reputacyjne. To właśnie banki są kanałem, przez który możliwe jest wsparcie polskiego i europejskiego systemu obronności przez kapitał prywatny. Sektor zbrojeniowy będzie pod wielką presją rozwoju i zaspokojenia zwiększonego popytu ze strony polskiego i innych rządów. Można oczekiwać, iż transakcje finansowe w tym sektorze, związane z napływem środków ze źródeł zewnętrznych, planowanymi wydatkami rządowymi, inwestycjami w przedsiębiorstwa, przepływami pieniężnymi będą gigantyczne. Konieczna będzie obsługa tych transakcji zarówno w aspekcie kredytowania, jak i zabezpieczenia transakcji zagranicznych (eksport polskiej produkcji, import). W szczególności **rola banków w rozwoju sektora obronnego w Polsce może dotyczyć następujących obszarów**:

1. Udzielanie kredytów inwestycyjnych przedsiębiorstwom z sektora zbrojeniowego w Polsce. Wskutek dużego napływu środków na zakup sprzętu produkowanego przez przedsiębiorstwa w Polsce, będą one potrzebować środków na rozwój, prace badawczo-rozwojowe. Ze względu na wielkość niezbędnego kapitału mogą to być kredyty konsorcjalne.

2. Obsługa transakcji (przepływów środków finansowych) związanych z zakupami sprzętu zbrojeniowego przez rząd Polski od przedsiębiorstw w Polsce i za granicą.

3. Zakup obligacji emitowanych przez SP i Fundusz Wsparcia Sił Zbrojnych (FWSZ). W Polsce wzrost wydatków rządowych na obronność ma swoje odzwierciedlenie w rosnącym długu publicznym i perspektywach dalszego jego wzrostu. Aby zapewnić stabilne finansowanie długoterminowe, należy albo zwiększyć deficyt albo – co jednak byłoby raczej trudne do realizacji politycznie – wprowadzić podatek zbrojeniowy/wojenny (tzw. *military tax*)[72] albo zwiększyć stawkę podatku VAT albo ograniczyć inne wydatki[73]. W takiej sytuacji państwo będzie zaciągać dług w postaci emisji obligacji, które mogą nabywać banki komercyjne i inne instytucje finansowe.

4. Zakup obligacji emitowanych przez przedsiębiorstwa z sektora obronnego.

5. Tworzenie funduszy inwestycyjnych skierowanych do start-upów (są to głównie MŚP), opracowujących nowe produkty, technologie typu dual-use. Fundusze te mogą zapewnić długookresową stabilność finansową.

6. Oferowanie usług dla *start-upów* opracowujących nowe produkty i technologie *dual-use* w zakresie pozyskiwania kapitału na rynkach zagranicznych.

7. Obsługa transakcji eksportu polskich produktów sektora zbrojeniowego.

71 https://commission.europa.eu/topics/defence/future-european-defence_en

72 Tego typu podatek wprowadziły np. Ukraina (w 2014 roku, który następnie znacząco podniesiono po rosyjskiej napaści w 2022 roku) oraz Estonia, gdzie począwszy od 1 lipca 2025 r. podniesiono o 2 pkt procentowe (z 22% do 24%) stawkę podatku VAT, co określono jako tymczasowy podatek wojenny w celu finansowania obrony, a od początku 2026 r. planowano wprowadzenie dodatkowego 2% podatku od dochodów osobistych oraz 2% podatku od dochodów firm (od zysków wypracowanych i dystrybuowanych). Te ostatnie podwyżki ostatecznie nie weszły w życie, ale podwyższono inne podatki, np. akcyzę na alkohol i energię.

73 Tego typu działania powinny oczywiście uwzględniać istniejące już obciążenia fiskalne zarówno w ujęciu ilościowym, jak i pod względem objęcia nimi poszczególnych grup podmiotów. Jak już wspominano, banki w Polsce, w przeciwieństwie do przedsiębiorstw innych sektorów, płacą już zwiększony CIT.

8. Oferowanie usług zabezpieczenia przed ryzykiem kursowym, by zminimalizować wpływ wahań kursowych na całkowity koszt finansowania z zagranicy.

4.3.3. Rola banków komercyjnych w finansowaniu inwestycji w energetykę, infrastrukturę

W UE, w tym w Polsce, inwestycje w sektor energetyczny są traktowane jako strategiczne i pożądane z kilku powodów: ochrony środowiska i klimatu – przejście na OZE, zapewnienia bezpieczeństwa geostrategicznego i niezależności energetycznej – bezpieczeństwo i pewność dostaw dla konsumentów i przemysłu, niskie koszty energii – dla konsumentów i przemysłu, co wpływa na konkurencyjność gospodarki. W przypadku zaangażowania środków państwa w takie inwestycje pojawia się kwestia pomocy publicznej, jej zgodności z przepisami UE i konieczności wydania zgody na dofinansowanie z budżetu.

W Polsce spodziewane są duże inwestycje w sektor energetyczny, w tym w OZE, elektrownie atomowe, modernizację infrastruktury energetycznej (w tym linii przesyłowych). To wymaga udziału polskich i zagranicznych podmiotów (finansowych, produkcyjnych) w skutecznym przeprowadzeniu transformacji energetycznej. Wydatki na rozwój sektora energetycznego (będącego własnością prywatną lub przedsiębiorstw z udziałem Skarbu Państwa) finansowane są z: środków własnych wypracowanych w przedsiębiorstwach, preferencyjnych programów oferowanych przez KE i publicznych środków (m.in. KPO – Fundusz Wsparcia Energetyki, którym zarządza Ministerstwo Klimatu i Środowiska we współpracy z BGK), kredytów zaciąganych w bankach komercyjnych. W ich finansowaniu niezbędna jest współpraca państwa (ministerstwa), spółek z udziałem SP (ARP, KUKE, spółki energetyczne), BGK oraz banków komercyjnych (krajowych i zagranicznych).

Z punktu widzenia banków komercyjnych finansowanie inwestycji w sektor energetyczny jest obarczone ryzykiem związanym z: długoterminowością inwestycji, wielkim zaangażowaniem kapitału, nieprzewidzialnymi zmianami regulacyjnymi w sektorze energetycznym i bankowym (pożądane są przewidywalność i stabilność regulacyjna), raportowaniem kwestii związanych ze zrównoważonym finansowaniem (pojawia się problem wiarygodności informacji uzyskanych od klientów o danym projekcie inwestycyjnym). Wysokość nakładów na transformację energetyczną wymusza też niejako wsparcie banków, które same nie są w stanie sfinansować takiego rzędu nakładów[74]. Stąd, konieczne jest połączenie środków unijnych, państwowych i prywatnych[75].

Z tych też powodów ważne są gwarancje państwa i jego agend. W tym kontekście warto wspomnieć o przygotowywanej (maj 2026 r.) przez Ministerstwo Finansów nowelizacji ustawy o poręczeniach i gwarancjach udzielanych przez Skarb Państwa oraz niektóre osoby prawne autorstwa. Ma ona na celu usprawnienie finansowania transformacji energetycznej, poprzez aktualizację przepisów dotyczących działalności poręczeniowej i gwarancyjnej Skarbu Państwa oraz Banku Gospodarstwa Krajowego.

4.3.4. Ryzyko odpływu depozytów

W latach 2019–2024 wydarzenia o charakterze geopolitycznym nie miały istotnego, negatywnego wpływu na poziom depozytów w polskim sektorze bankowym. W analizowanym okresie depozyty wykazywały stabilną tendencję wzrostową, co ilustruje Wykres 27. Oznacza to, że zarówno pandemia COVID-19, jak i eskalacja ryzyka geopolitycznego po wybuchu wojny w Ukrainie nie doprowadziły do masowego odpływu środków z banków ani do materializacji ryzyka płynnościowego po stronie sektora bankowego.

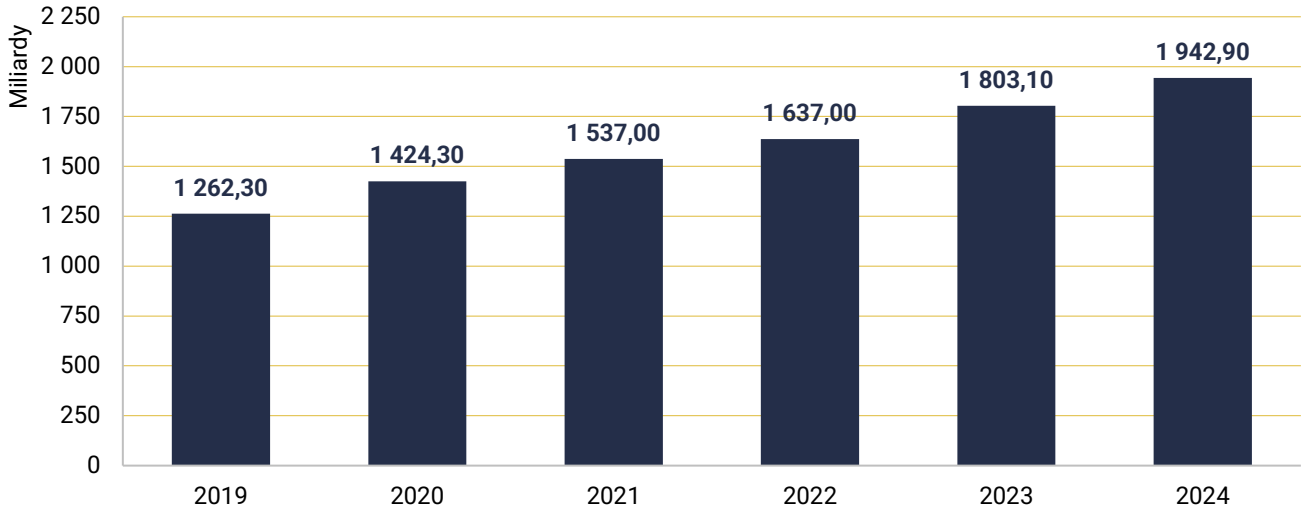
W okresie pandemii, pomimo gwałtownego wzrostu gotówki w obiegu o około 35 procent wiosną 2020 roku, głównym wyzwaniem dla sektora bankowego nie było ryzyko płynnościowe, lecz wzrost ryzyka kredytowego wynikający z pogorszenia sytuacji ekonomicznej gospodarstw domowych i przedsiębiorstw. Ryzyko to zostało istotnie złagodzone dzięki działaniom Narodowego Banku Polskiego, polegającym na zapewnieniu bankom odpowiedniego dostępu do płynności oraz złagodzeniu

74 Szacuje się, że łączny koszt transformacji energetycznej do 2040 roku może wynieść od 1,5 do 1,7 biliona PLN. (https://www.bgk.pl/dla-klienta/strefa-wiedzy-bgk/artykul/transformacja-energetyczna-w-polsce...). Wydatki obejmą przede wszystkim: • modernizację i rozbudowę sieci przesyłowych i dystrybucyjnych (ok. 400–500 mld zł), • rozwój odnawialnych źródeł energii oraz magazynów, w tym elektrowni szczytowo-pompowych (ok. 600 mld zł), • budowę bloku jądrowego (ok. 200 mld zł), • transformację sektora ciepłowniczego (ok. 450 mld zł).

75 Polska otrzymała ponad 42 mld zł z programów unijnych FEnIKS i FEPW na transformację energetyczna, z czego na koniec kwietnia 2026 roku zakontraktowano już niemal 70% środków.

warunków obsługi zadłużenia. Efekt ten osiągnięto między innymi poprzez obniżenie stóp procentowych, co przełożyło się na spadek wysokości rat kredytów i ograniczenie presji na jakość portfela kredytowego (Szczepańska, 2022).

Wykres 27. Poziom depozytów sektora niefinansowego w polskim sektorze bankowym (mld PLN)

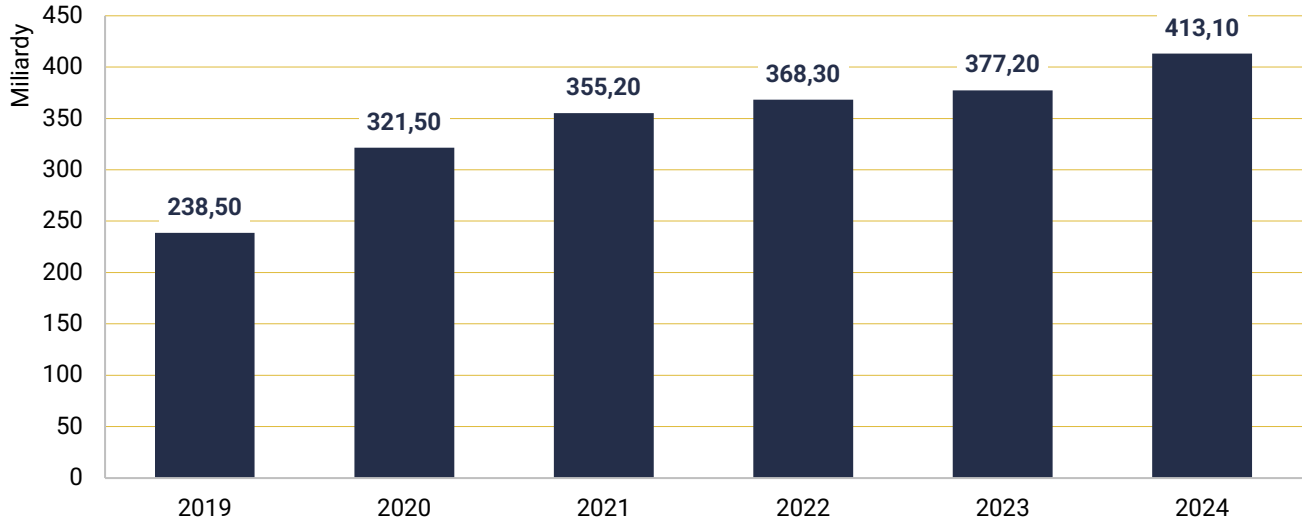


Źródło: Opracowanie własne na podstawie (NBP 2024, 2025B).

Narodowy Bank Polski w raporcie „Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2020 r." wskazuje, że wzrost gotówki w obiegu w pierwszej fazie pandemii miał w dominującym stopniu charakter tezauryzacyjny i przezornościowy, a nie transakcyjny. W pierwszym półroczu 2020 roku klienci banków rzadziej podejmowali gotówkę z bankomatów, ale towarzyszył temu wzrost średniej kwoty wypłat. W celu zapewnienia dostępności gotówki, operatorzy bankomatów wprowadzili czasowe ograniczenie maksymalnej kwoty pojedynczej transakcji do 1000 zł (Narodowy Bank Polski, 2020).

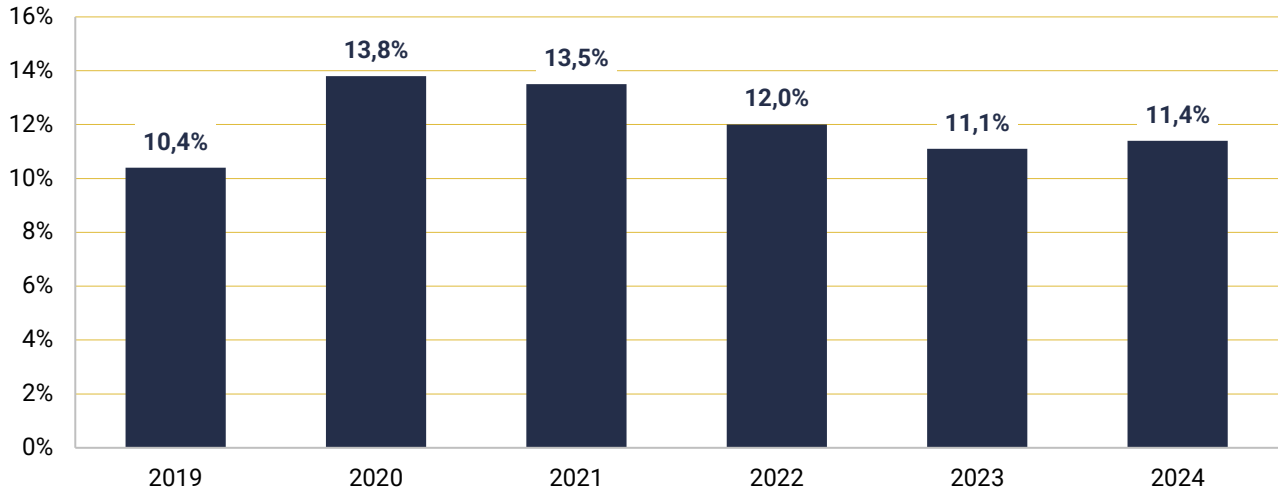
Od 2021 r. nie obserwowano już dynamiki wzrostu gotówki w obiegu porównywalnej z początkiem pandemii, co ilustruje Wykres 28. Dodatkową perspektywę wnosi relacja wartości gotówki w obiegu do PKB (Wykres 29). Między 2019 a 2020 rokiem nastąpił gwałtowny wzrost tego wskaźnika z poziomu 10,4% do 13,8%, co odzwierciedla istotny wzrost popytu na gotówkę w warunkach niepewności pandemicznej. W kolejnych latach wskaźnik stopniowo malał, stabilizując się w 2023–2024 r. nieco powyżej 11%, co wskazuje na częściową normalizację po okresie pandemii, przy utrzymaniu relatywnie wyższej niż przed 2020 r. roli gotówki w gospodarce.

Wykres 28. Wartość gotówki w obiegu w Polsce w latach 2019–2024 (mld PLN)



Źródło: Opracowanie własne na podstawie (NBP, 2021a, 2023, 2025a).

Wykres 29. Wartość gotówki w obiegu w relacji do PKB w latach 2019–2024

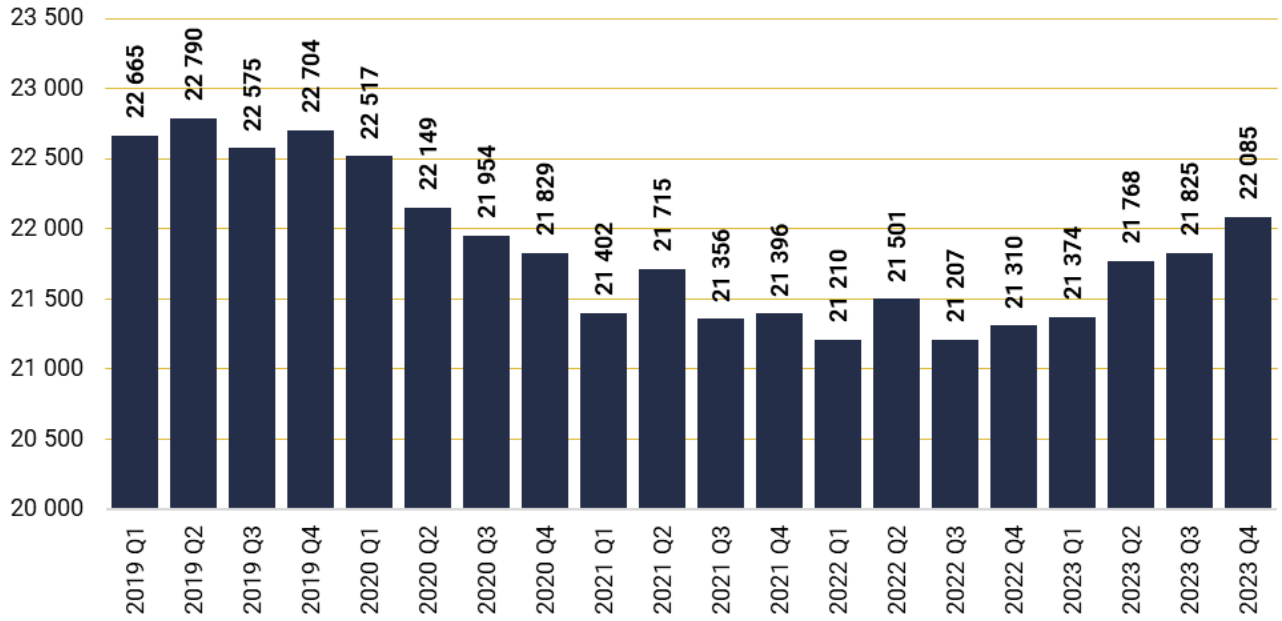


Źródło: Opracowanie własne na podstawie (NBP, 2021a, 2023, 2025a).

W Polsce wyłączne prawo emitowania banknotów i monet waluty polskiej posiada Narodowy Bank Polski. Nie oznacza to jednak automatycznie niezakłóconego dostępu do gotówki w sytuacji podwyższonej niepewności, ponieważ ograniczeniem bywa nie obecność gotówki w ujęciu systemowym, lecz przepustowość kanałów jej dystrybucji. Z tego punktu widzenia kluczowe znaczenie ma infrastruktura gotówkowa obejmująca sieć oddziałów i urządzeń samoobsługowych oraz podmioty realizujące fizyczne procesy obsługi gotówki (transport, przeliczanie, sortowanie, przechowywanie), określane zbiorczo jako firmy CIT. W praktyce uczestniczą one w realizacji cyklu zaopatrywania rynku w gotówkę, dlatego w warunkach nagłego wzrostu popytu mogą pełnić rolę operacyjnego „wąskiego gardła" dostępności gotówki w konkretnych lokalizacjach.

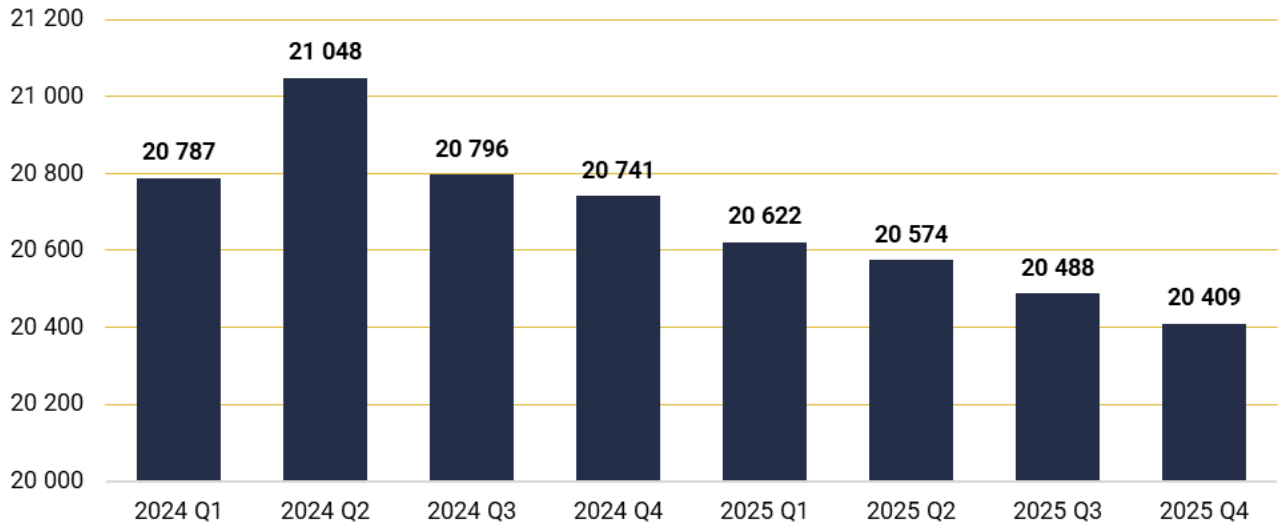
Z perspektywy dostępności gotówki w sytuacji kryzysowej istotny jest systematyczny spadek liczby placówek bankowych. Na koniec 2019 r. sieć bankowa obejmowała 6 115 oddziałów oraz 3 237 filii, ekspozytur i innych placówek obsługi klienta, natomiast na koniec 2024 r. sieć bankowa obejmowała 4 953 oddziały oraz 2166 filii, ekspozytur i innych placówek obsługi klienta. Oznacza to redukcję sieci z poziomu ponad 9 tys. do nieco ponad 7 tys. w horyzoncie 2019–2024.

Wykres 30. Liczba bankomatów w latach 2019–2023 (ujęcie kwartalne)



Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/bankomaty.xlsx.

Wykres 31. Liczba bankomatów w latach 2024–2025 (ujęcie kwartalne)



Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/bankomaty.xlsx.

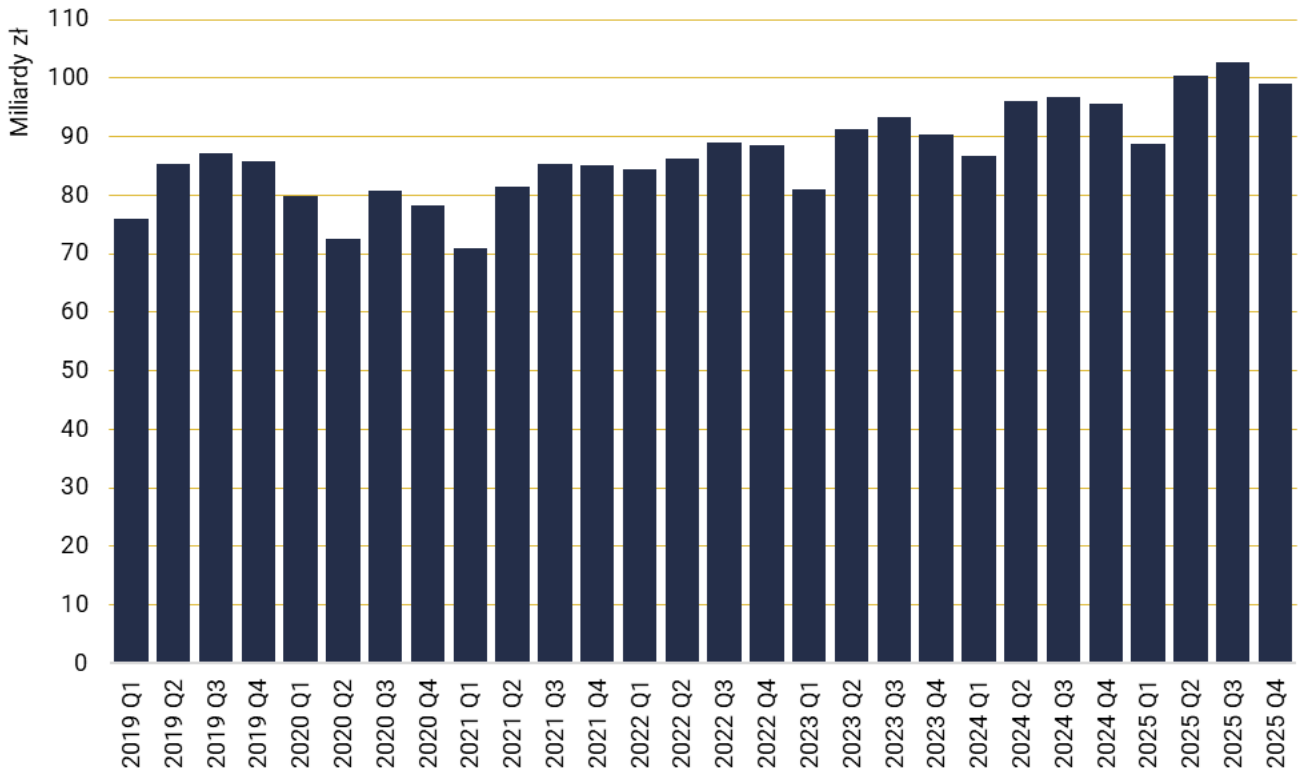
Równolegle nie nastąpił trwały wzrost infrastruktury bankomatowej (NBP, 2020, 2025). Liczbę bankomatów w latach 2019–2023 oraz 2024–2025 przedstawiono odpowiednio na wykresach 12–13. Należy podkreślić, iż dane o liczbie bankomatów do 2023 r. nie są porównywalne z danymi w kolejnych latach (stąd rozbicie na dwa osobne wykresy) z uwagi na zmianę metodyki zbierania i opracowywania danych o tych urządzeniach. Z początkiem 2024 r. nałożono obowiązek sprawozdawczy na operatorów bankomatów, co pozwoliło na wyeliminowanie podwójnego raportowania niektórych urządzeń i niejako urealniło statystyki bankomatów.

W konsekwencji opisanych tendencji rośnie, sygnalizowane wcześniej, znaczenie odpornej logistyki zaopatrzenia w gotówkę, w tym zdolności do szybkiego zwiększenia tempa zasileń bankomatów w sytuacji lokalnych szoków informacyjnych lub zdarzeń o charakterze kinetycznym/hybrydowym. Z tego względu zasadne jest, aby sektor bankowy kontraktowo wymagał od firm CIT i pozostałych podmiotów łańcucha dostaw gotówki utrzymywania planów ciągłości działania, procedur awaryjnych zasileń bankomatów, rozwiązań alternatywnych dla kluczowych tras i zasobów, zdolności wykorzystania zapasowych centrów gotówkowych oraz sprawnego raportowania incydentów i ograniczeń operacyjnych.

Problem nagłego, nieprzewidzianego wzrostu zapotrzebowania na gotówkę oraz sytuacji nadzwyczajnych w procesie zaopatrywania rynku w gotówkę został zaadresowany przez NBP w Narodowej Strategii Bezpieczeństwa Obrotu Gotówkowego, co sprzyjało budowaniu odporności sektora bankowego na szoki, w tym również mające podłoże geopolityczne (w tym te o charakterze „czarnych łabędzi"). Na potrzeby tej strategii przyjęto kryterium dostępności gotówki zakładające zapewnienie 90% populacji w Polsce dostępu do najbliższego oddziału banku z obsługą kasową lub bankomatu w odległości nie większej niż 10 km. Ponadto analizie poddano alternatywne sposoby dostępu do gotówki, w szczególności usługę *cashback* w punktach handlowo-usługowych wyposażonych w terminale płatnicze, wykorzystanie infrastruktury Poczty Polskiej oraz rozwiązania typu CashTech, umożliwiające wypłatę gotówki z kasy sklepowej przy okazji płatności za pomocą aplikacji bankowej. NBP zaproponował także rozwój systemu depozytowego w kierunku depozytu dwustronnego, który miałby dopuścić przechowywanie depozytu NBP w pomieszczeniach firm CIT oraz zasilanie depozytu NBP przez banki i Pocztę Polską gotówką pochodzącą z rynku. W obszarze bezpieczeństwa fizycznego Strategia wskazuje rekomendowane obszary, dla których należy wypracować zestaw dobrych praktyk, takie jak ochrona obiektów i urządzeń przechowujących gotówkę, bezpieczeństwo odbioru i wydawania znaków pieniężnych, przeliczanie gotówki, szkolenia personelu, transport i wyposażenie pojazdów, informatyzacja i automatyzacja procesów, trasy transportu oraz zarządzanie procesami obsługi gotówki (Narodowy Bank Polski, 2021).

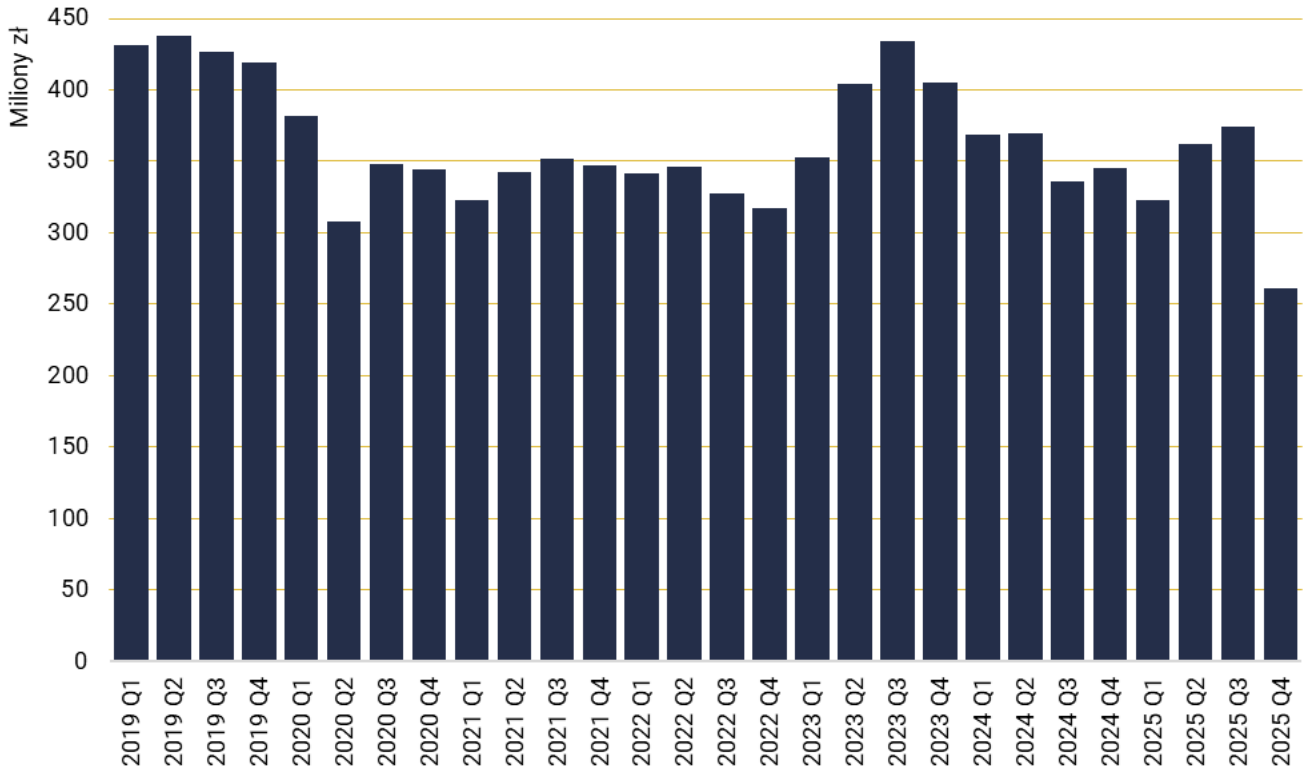
Rezultatem podjętych działań i funkcjonujących rozwiązań systemowych był niezakłócony proces zaopatrywania gospodarki w gotówkę. Infrastruktura sektora bankowego okazała się wydolna, także w obliczu wzrostu popytu na pieniądz gotówkowy (zgłaszanego nie tylko z uwagi na motyw transakcyjny, ale i – w coraz większym stopniu – motyw przezornościowy). Zilustrowano to na wykresach odnoszących się do okresu od wybuchu pandemii COVID-19 do końca 2025 r.

Wykres 32. Bankomaty – wypłaty w kraju w latach 2019–2025



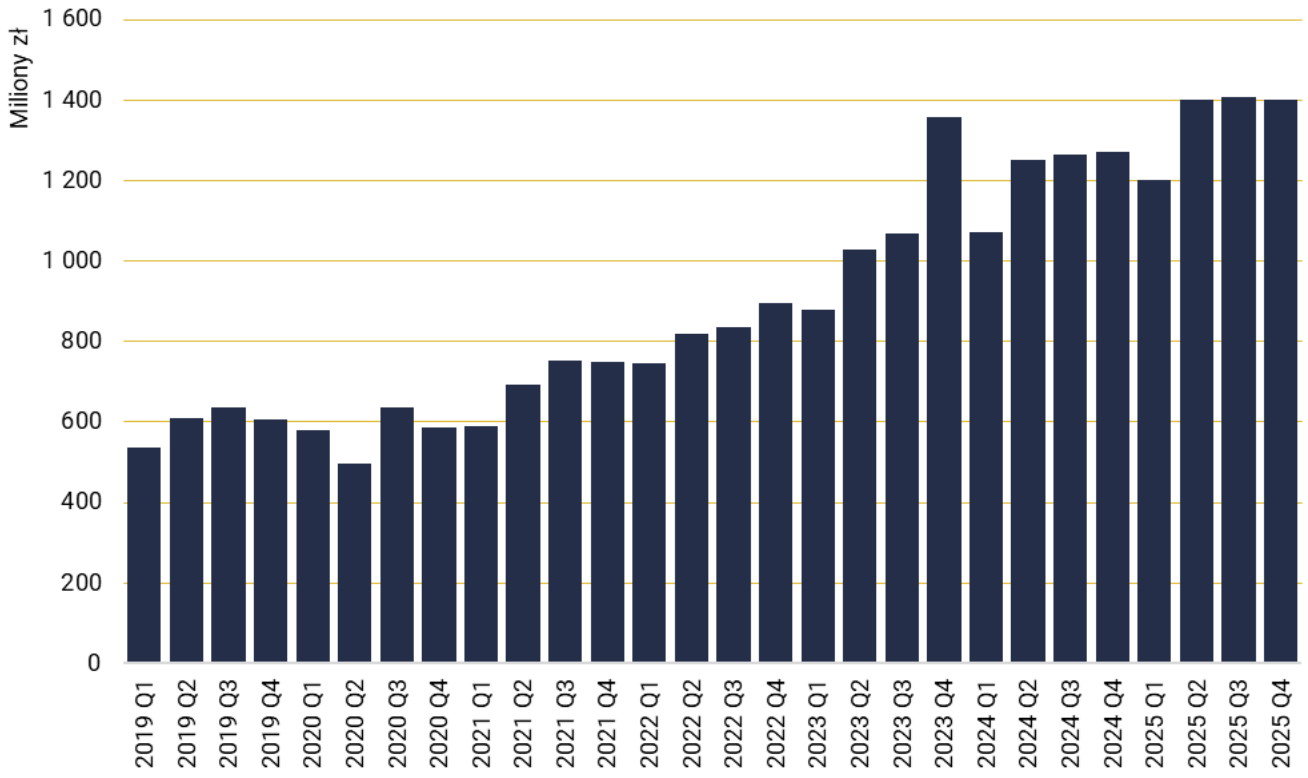
Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/transakcje_wartosc.xlsx.

Wykres 33. Wypłaty z kas banków w latach 2019–2025



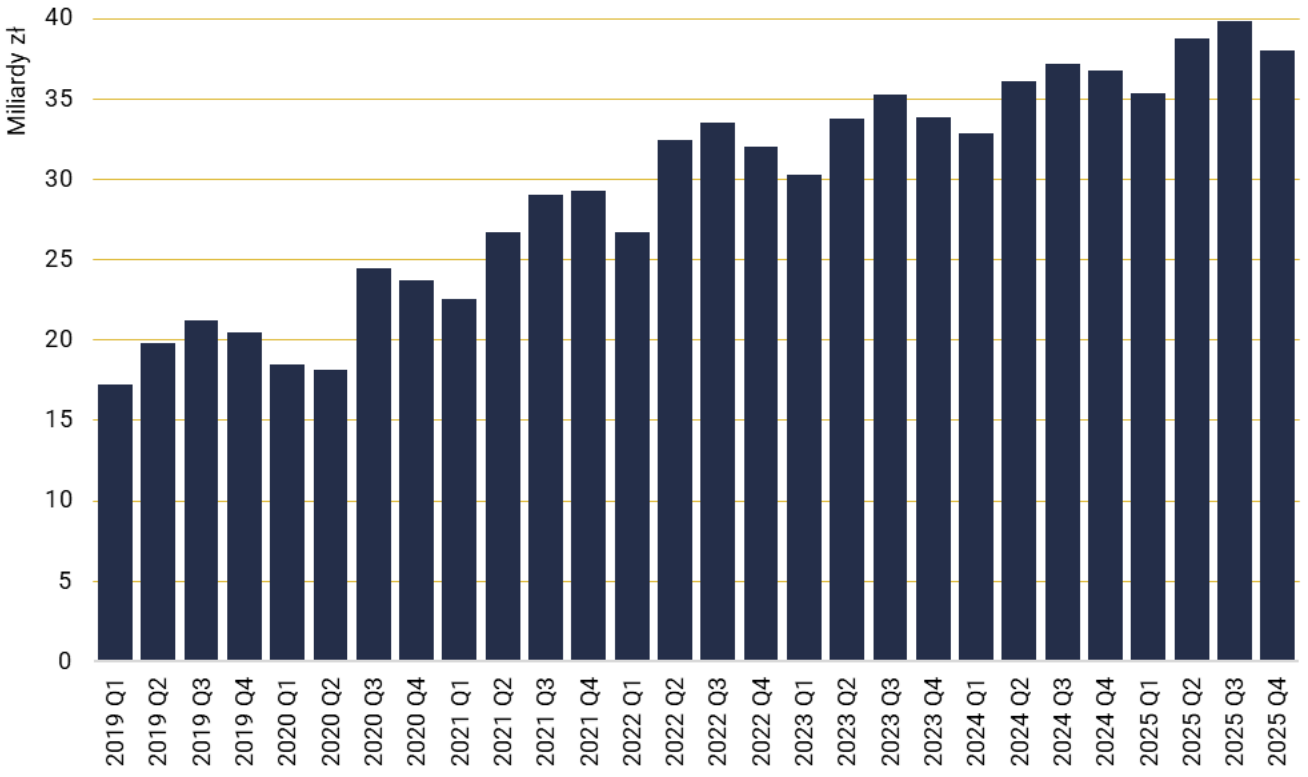
Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/transakcje_wartosc.xlsx.

Wykres 34. Wypłaty sklepowe w latach 2019–2025



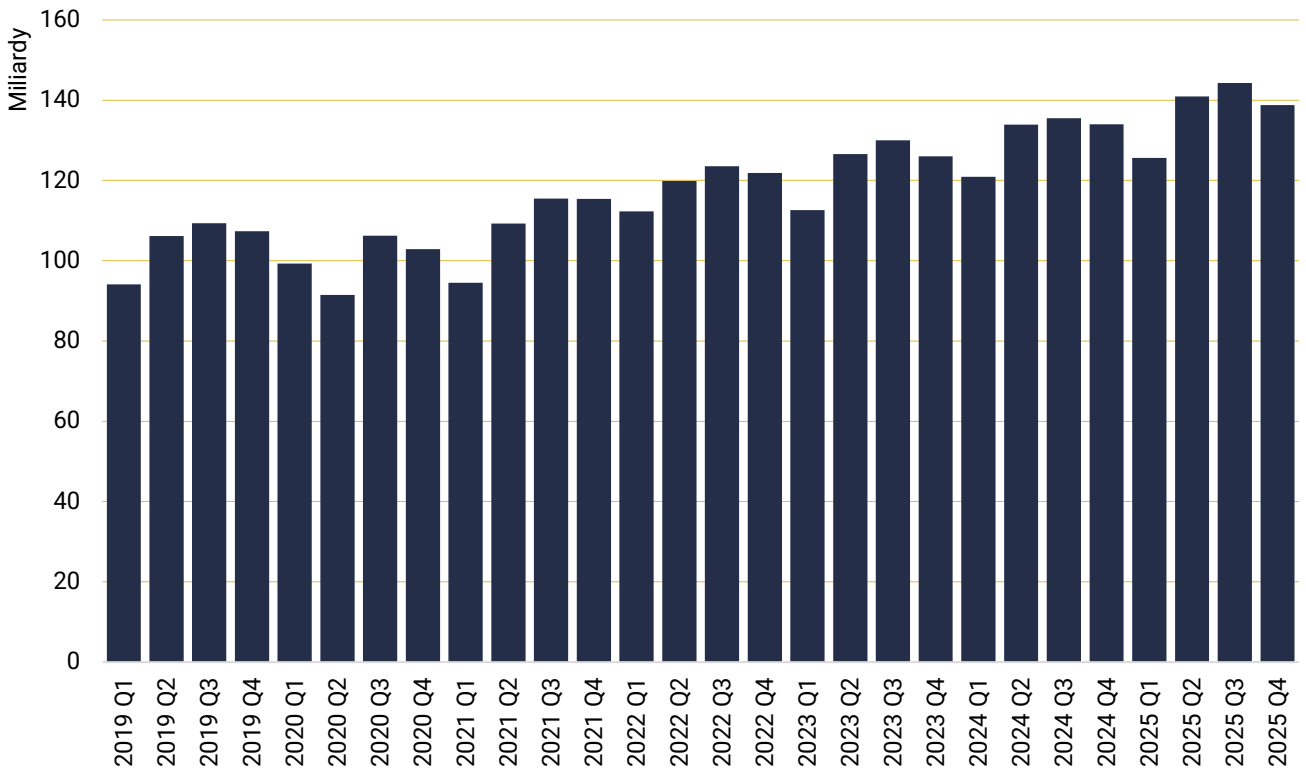
Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/transakcje_wartosc.xlsx.

Wykres 35. Inne wypłaty krajowe w latach 2019–2025



Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/transakcje_wartosc.xlsx.

Wykres 36. Łączne wypłaty gotówkowe w kraju w latach 2019–2025



Źródło: Opracowanie własne na podstawie: https://static.nbp.pl/systemy/platniczy/transakcje_wartosc.xlsx.

4.3.5. Komunikacja kryzysowa i ryzyko reputacyjne w warunkach wojny informacyjnej

Obecna sytuacja geopolityczna, charakteryzująca się rosnącym napięciem i działaniami balansującymi na granicy otwartego konfliktu, w połączeniu ze zwiększoną aktywnością cyberprzestępców, potęguje ryzyko ataków informacyjnych. Ich integralnym elementem są działania z zakresu wojny informacyjnej oraz działania hybrydowe (European Council, 2024). Celem adwersarzy często bywa wywołanie określonych reakcji społecznych zgodnych z ich wrogimi intencjami, takich jak podważenie zaufania do instytucji publicznych czy paraliż infrastruktury krytycznej, w tym sektora finansowego (Instytut Cyberbezpieczeństwa, 2024).

W ramach wojny informacyjnej wyróżnić można ataki wykorzystujące misinformację, dezinformację oraz malinformację (MDM). Misinformacja to treści nieprawdziwe, ale rozpowszechniane bez złych intencji. Dezinformacja polega na celowym tworzeniu fałszywych treści, które mają kształtować szkodliwe postawy społeczne lub przynieść korzyści adwersarzom. Z kolei malinformacja to rozpowszechnianie informacji prawdziwych, lecz użytych w szkodliwym kontekście. W operacjach informacyjnych malinformacja (często w formie półprawd) może stanowić podbudowę dla działań dezinformacyjnych, uwiarygadniając nadawcę, który w kolejnym etapie wprowadza odbiorców w błąd (NASK, 2025).

Przykładem silnego, negatywnego oddziaływania zjawisk z obszaru MDM na sektor finansowy są incydenty, które dotknęły brytyjski Metro Bank w 2019 roku oraz amerykański Silicon Valley Bank (SVB) w 2023 roku. W przypadku Metro Bank sprawcy posłużyli się plotką (malinformacją) rozpowszechnianą za pośrednictwem komunikatora WhatsApp. Treść wiadomości sugerowała problemy z płynnością finansową i gwałtowny spadek zaufania inwestorów. Autorzy plotki wzywali do natychmiastowego wycofania oszczędności, powołując się na prawdziwy artykuł, który opisywał realne trudności banku z pozyskaniem kapitału oraz znaczny spadek wyceny giełdowej tej spółki. Wykorzystanie wiarygodnego źródła w alarmistycznym kontekście sprawiło, że klienci masowo ruszyli do placówek, by wypłacić depozyty (Edwards, 2019). Wyżej opisany mechanizm jest o tyle groźny, że plotka, krążąc poza przestrzenią publiczną, utrudniła szybką reakcję i kontrnarrację ze strony banku.

Z kolei upadek Silicon Valley Bank, instytucji kluczowej dla amerykańskiego sektora startupów,

przyspieszyła panika informacyjna w mediach społecznościowych. Dyskusja na platformie Twitter (obecnie X), dotycząca płynności banku i bezpieczeństwa środków, wywołała lawinową reakcję klientów – tylko pierwszego dnia wypłacono 42 miliardy dolarów (Korn, 2023). Choć przypadek Silicon Valley Bank nie stanowi bezpośredniego przykładu celowej wojny informacyjnej, doskonale ilustruje on siłę oraz tempo oddziaływania mediów społecznościowych na sektor finansowy. W tej sytuacji błyskawicznie rozprzestrzeniająca się misinformacja (wynikająca raczej z obaw, a nie ze złych intencji nadawców) doprowadziła w konsekwencji do upadku tej instytucji. Badania zainspirowane tym incydentem wykazały, że publiczne dyskusje o kondycji finansowej banków w mediach społecznościowych silnie wzmacniają zjawisko runu na bank. Co istotne, efekt ten dotyczy nie tylko instytucji będącej bezpośrednim obiektem dyskusji, ale może przenosić się na pozostałe banki, generując ryzyko systemowe (Cookson i in., 2023).

Zdaniem przedstawicieli Europejskiego Banku Centralnego (Tuominen, 2025), ryzyko związane z atakami informacyjnymi staje się elementem bazowego scenariusza zagrożeń dla systemu bankowego. Na wzrost tego ryzyka wpływa błyskawicznie postępująca cyfryzacja sektora oraz eskalacja napięć geopolitycznych, w których cyberataki wykorzystywane są do osiągania celów politycznych. Tuominen (2025) zauważa, że bieżące środki zaradcze stosowane przez banki są niewystarczające w praktyce, aby skutecznie zaadresować ryzyka związane z atakami informacyjnymi. W szczególności w odniesieniu do planów komunikacji kryzysowej z klientami w przypadku wystąpienia ataku informacyjnego.

W raporcie 25/13MFW (2025), podobnie jak w opracowaniu Tuominen (2025), wskazuje się na wzrost ryzyka ataku informacyjnego na sektor finansowy. Tego rodzaju atak, ze względu na silne powiązania oraz korzystanie przez banki z usług tych samych kluczowych zewnętrznych dostawców (CTPP), może mieć charakter systemowy i ulegać transmisji między bankami, np. wywołując run na instytucje niebędące bezpośrednim celem ataku.

Pomimo zidentyfikowania regulacji wspomagających redukcję ryzyka związanego z atakami informacyjnymi, MFW zwraca uwagę na problemy z ich wdrażaniem i uznaje je za niewystarczające. Raport 25/213 podkreśla, że krajowe organy nadzorcze (NCA) poszczególnych państw członkowskich UE korzystają z różnych rozwiązań informatycznych, które nie zawsze są zintegrowane z systemami organów pozostałych państw członkowskich. MFW wskazuje na konieczność wdrożenia i praktycznego przetestowania ogólnoeuropejskich ram koordynacji odpowiedzi na systemowe cyberincydenty (EU-SCICF), zaproponowanych przez Europejską Radę ds. Ryzyka Systemowego (ESRB). Zgodnie z założeniami, wprowadzenie EU-SCICF ma zapobiec chaosowi informacyjnemu w przypadku transgranicznego incydentu informatycznego o charakterze systemowym (Europejska Rada ds. Ryzyka Systemowego, 2021).

Dokumenty opisujące problem paniki i runu na banki wywołanego szokiem informacyjnym, opracowane na potrzeby Banku Rozrachunków Międzynarodowych (BIS), wskazują, że szok informacyjny może uruchomić kaskadę wycofywania depozytów i utraty reputacji przez banki (Sandri i in., 2023). Badanie przeprowadzone na potrzeby BIS w 2023 roku na próbie ponad 6 000 Amerykanów pokazuje, że ankietowani mają niską świadomość dotyczącą bezpieczeństwa depozytów (prawie 50% z nich nie wie, jaka jest maksymalna kwota gwarantowanych depozytów, a ponad 50% nie zna ratingu amerykańskich banków). Autorzy badania wskazują, że depozytariusze reagują na podwyższone ryzyko w sektorze bankowym, wycofując depozyty (około 1/3 wycofanych depozytów lokowana jest w innych bankach, a pozostała część przechowywana jest głównie w postaci gotówki, przy czym zakup aktywów inwestycyjnych jest niewielki).

W przytoczonym badaniu pokazano również, że spójna, oparta na faktach komunikacja ze strony organów bankowych (np. SRF) ma silniejsze oddziaływanie na powstrzymanie runu na banki niż komunikaty polityków, które trafiają głównie do ich wyborców. Wynika z tego, że skuteczniejszym narzędziem ograniczania paniki wśród depozytariuszy są spójne komunikaty płynące z sektora bankowego i organów nadzorczych, a nie próby uspokajania nastrojów i wchodzenie w polemiki z dezinformacją.

Przykładem konsekwentnej polityki antydezinformacyjnej może być Narodowy Bank Ukrainy (NBU), który skutecznie walczy z dezinformacją na temat stabilności ukraińskiego systemu finansowego, m.in. przez wydawanie merytorycznych raportów pokazujących stan ukraińskiego sektora finansowego wraz z mechanizmami jego obrony (NBU, 2022) oraz na bieżąco dementując (z podaniem podstawy prawnej oraz aktualnych danych) dezinformacje pojawiające się w mediach społecznościowych.

Obecne regulacje prawne mające chronić banki przed cyberatakami, w tym przed dezinformacją, są zdefiniowane na dość wysokim poziomie ogólności. Wciąż brakuje jasnych wytycznych operacyjnych, które mogłyby stanowić wskazówki dla banków w sytuacji, w której dezinformacja wpływa na skłonność depozytariuszy do wycofywania środków z sektora bankowego. W przypadku walki z dezinformacją moż-

na odnieść się do podobnego problemu dotyczącego wpływu dezinformacji na przebieg wyborów, który zaadresowała amerykańska Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) w przewodniku dla urzędników przeprowadzających wybory (Cybersecurity and Infrastructure Security Agency, 2022). CISA zaproponowała pięcioetapowy model TRUST, którego celem jest wzmocnienie organizacyjnej odporności na ataki informacyjne. Model ten składa się z następujących etapów:

1. *Tell Your Story* – przygotowanie rzetelnego opisu organizacji z wyprzedzeniem, zanim pojawią się ataki informacyjne. Etap ten obejmuje cykliczną edukację interesariuszy (klientów, pracowników, akcjonariuszy) w zakresie kondycji organizacji, branży i wymogów regulacyjnych. Działania edukacyjne powinny korzystać ze sprawdzonych i aktualnych danych. Interesariusze powinni znać wdrożone przez bank procedury i mechanizmy ochronne (np. gwarancje depozytów, ubezpieczenia, reasekurację). Na tym etapie warto przewidzieć możliwe narracje dezinformacyjne i przygotować protokoły reakcji gotowe do szybkiego wdrożenia. Dobre relacje z mediami ułatwiają szybkie przekazanie spójnych komunikatów i ograniczają chaos informacyjny.

2. *Ready Your Team* – przygotowanie organizacji do odpowiedzi na potencjalny incydent informacyjny. W tym etapie zalecane jest powołanie dedykowanej jednostki odpowiedzialnej za bieżące przygotowywanie i aktualizowanie protokołów reakcji oraz ich szybkie wdrożenie. CISA zaleca też ustanowienie wiarygodnych kanałów komunikacji, w tym publikowanie komunikatów w mediach społecznościowych z wykorzystaniem zweryfikowanych kont. Równie ważna, jak spójne komunikaty, jest zdolność do obsługi licznych indywidualnych zapytań kierowanych różnymi kanałami (telefon, e-mail, media społecznościowe).

3. *Understand and Assess* – rozpoznanie i ocena siły wpływu ataków informacyjnych na organizację. W tym etapie powinno się ocenić realny wpływ zagrożeń na działalność organizacji oraz oszacować możliwe szkody, w oparciu o zidentyfikowane wcześniej scenariusze. CISA rekomenduje monitorowanie treści dotyczących organizacji w przestrzeni publicznej i internecie. W zależności od charakteru wykrytych treści należy zareagować albo kontynuować monitorowanie.

4. *Strategize Response* – dobór zakresu, skali i środka przekazu dla odpowiedzi stosownie do charakteru zagrożenia informacyjnego. CISA podkreśla, że nie każdy atak informacyjny wymaga natychmiastowej reakcji ani użycia wszystkich kanałów komunikacji. Kluczowe jest dopasowanie komunikatu do odbiorców (kim są, jak silnie zostali dotknięci dezinformacją, jakie mają potrzeby informacyjne i z jakich kanałów korzystają). Wśród dobrych praktyk komunikacji kryzysowej CISA wskazuje: opieranie przekazu na faktach, zwięzłość i konkret, unikanie polemiki z treściami dezinformacyjnymi oraz współpracę z partnerami sektorowymi w celu zapewnienia spójności komunikatów.

5. *Track Outcomes* – analiza rozwoju sytuacji po odpowiedzi na atak. CISA zaznacza, że nawet dobrze przygotowana i skrupulatnie przeprowadzona reakcja nie musi zakończyć ataku. Szkodliwe narracje potrafią ewoluować na inne kanały i tematy, dlatego organizacja powinna ciągle monitorować przestrzeń publiczną i internet, aby wcześnie wykrywać zmiany i we współpracy z partnerami sektorowymi odpowiednio dostosowywać działania. Na tym etapie należy także rzetelnie ocenić podjęte działania i wprowadzić poprawki do protokołów reagowania.

Model TRUST, mimo że nie jest dedykowany dla sektora bankowego, prezentuje dobre praktyki walki z dezinformacją. Kluczowe w tym modelu jest przygotowanie organizacji na potencjalny atak (protokoły, wzorce odpowiedzi, kanały), aby uniknąć chaosu informacyjnego. W sektorze bankowym największym ryzykiem nie jest sama dezinformacja, lecz chaos informacyjny, który może podważyć zaufanie i reputację, a w konsekwencji doprowadzić do odpływu depozytów. Z uwagi na powyższe ryzyko zasadne jest opracowanie sektorowego protokołu reagowania na atak informacyjny, koordynowanego w ramach Związku Banków Polskich, z uwzględnieniem roli Narodowego Banku Polskiego jako źródła faktów i zaufania. Współpraca banków w zakresie ujednolicenia kanałów komunikacji oraz powiązania z mechanizmami EU-SCICF ma znaczenie dla odporności systemu bankowego w ujęciu ogólnoeuropejskim.

4.3.6. Ekosystem reagowania na atak informacyjny

Sprawne funkcjonowanie sektorowego protokołu reagowania na atak informacyjny wymaga nie tylko procedur, lecz także operacyjnie i prawnie umocowanego ekosystemu informacyjnego. Doświadczenia amerykańskie i ukraińskie, a także rekomendacje formułowane na poziomie europejskiego nadzoru

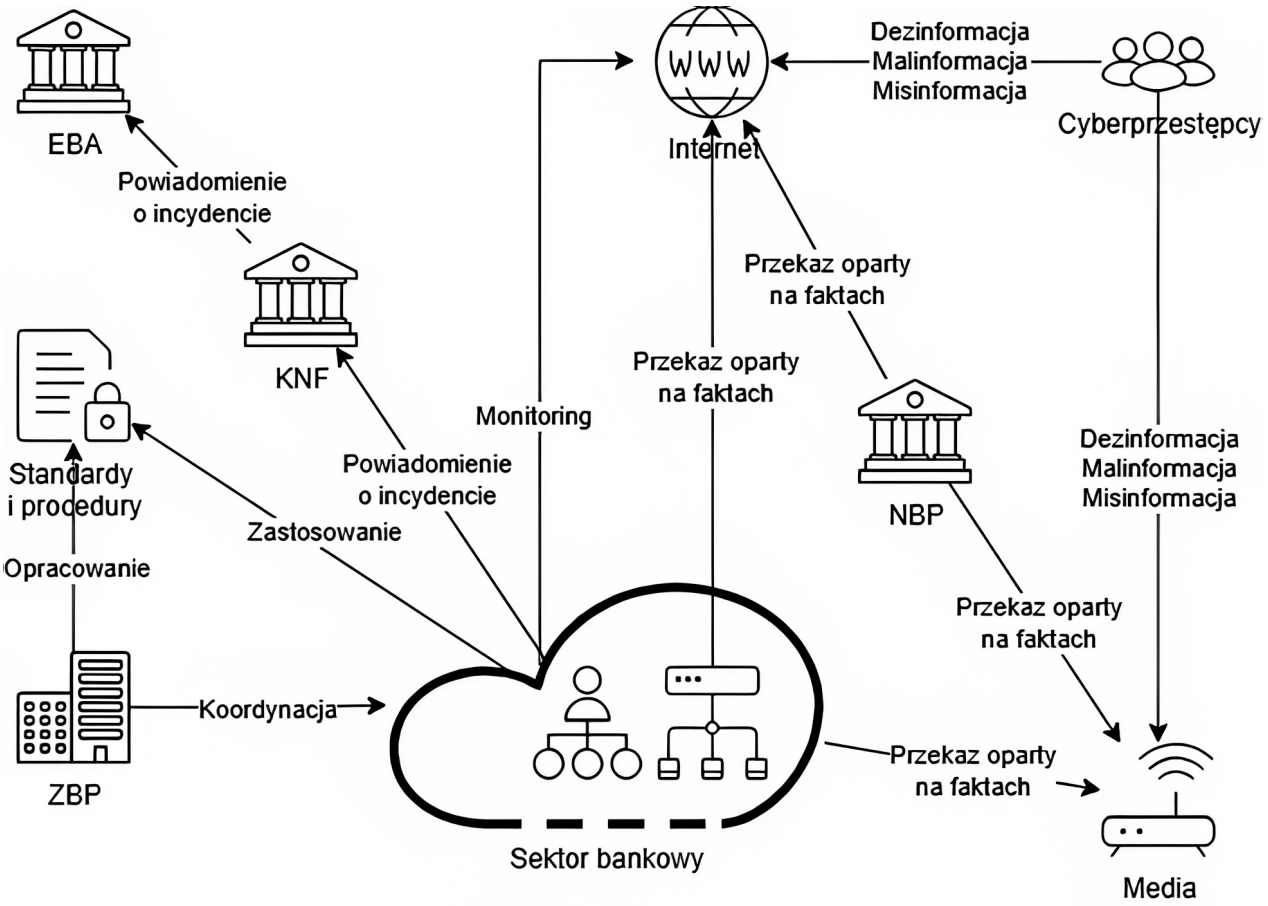
bankowego wskazują, że odporność komunikacyjna musi być budowana systemowo, w oparciu o stałe mechanizmy wymiany informacji i spójne kanały przekazu.

Ze względu na ryzyko transmisji zagrożeń informacyjnych między instytucjami finansowymi kluczowym elementem takiego ekosystemu powinna być ciągła i ustrukturyzowana wymiana informacji pomiędzy bankami, obejmująca zarówno identyfikowane narracje, jak i ich dynamikę, zasięg oraz kanały dystrybucji. Banki komercyjne powinny rozważyć wspólną budowę i utrzymanie infrastruktury, na przykład w modelu chmury hybrydowej, która umożliwi bieżące gromadzenie danych z monitoringu internetu i mediów, w szczególności mediów społecznościowych, oraz ich analizę z wykorzystaniem narzędzi do przetwarzania dużych zbiorów danych i identyfikacji powiązań pomiędzy treściami, źródłami i odbiorcami.

Naturalnym koordynatorem współpracy w tym obszarze wydaje się Związek Banków Polskich, który mógłby pełnić rolę platformy uzgadniania standardów i procesów, w tym sektorowego protokołu reagowania na ataki informacyjne, a także organizacji ćwiczeń i testów gotowości. Równolegle do monitoringu, krytycznym zadaniem ekosystemu jest wytwarzanie spójnego, rzetelnego i audytowalnego przekazu, opartego na dokumentach, prawie i procedurach, a nie na polemice z narracjami dezinformacyjnymi. W tym miejscu szczególną rolę odgrywa bank centralny, który, dołączając do komunikacji i uwiarygadniając ją swoim autorytetem, wzmacnia jej oddziaływanie w warunkach podwyższonej niepewności. Przekaz banków powinien być dystrybuowany wielokanałowo i adresowany do wszystkich kluczowych mediów oraz grup interesariuszy, niezależnie od tego, w którym kanale pierwotnie pojawił się atak informacyjny, tak aby ograniczać chaos informacyjny i minimalizować ryzyko eskalacji paniki. Ponadto w ramach ekosystemu reagowania należy zapewnić niezwłoczne przekazanie informacji o wykrytym incydencie do Komisji Nadzoru Finansowego, która w razie potrzeby może uruchomić dalszą wymianę informacji na poziomie europejskim, w tym z Europejskim Urzędem Nadzoru Bankowego (EBA).

Przykładową architekturę ekosystemu reagowania na ataki informacyjne przedstawiono na Rysunku 5. Ilustracja identyfikuje kluczowych aktorów ekosystemu, wykorzystywane kanały komunikacji oraz relacje i przepływy informacji zachodzące pomiędzy nimi.

Rysunek 5. Architektura ekosystemu reagowania na atak informacyjny



Źródło: *Opracowanie własne.*

Na podstawie modelu TRUST oraz dobrych praktyk wynikających z podejścia EU-SCICF opracowano sektorowy protokół reagowania na atak informacyjny. Protokół obejmuje dwa tryby działania: niekryzysowy oraz kryzysowy. Tryb niekryzysowy charakteryzuje się cyklicznością i ciągłością działań. Tryb kryzysowy uruchamiany jest na poziomie incydentu lokalnego w pojedynczym banku, który charakteryzuje się możliwością eskalacji do poziomu sektorowego.

Tryb niekryzysowy obejmuje:

1. Opracowanie dokumentów, standardów oraz ekosystemu reagowania na ataki informacyjne. W ramach prac koordynowanych przez ZBP banki uzgadniają standardy dotyczące opisu, przechowywania, przetwarzania, udostępniania oraz bezpiecznego przesyłania informacji i dokumentów wykorzystywanych w reagowaniu na ataki informacyjne. Pożądane jest utworzenie ekosystemu reagowania na ataki informacyjne w postaci wspólnej infrastruktury, na przykład chmury hybrydowej, z którą banki zintegrowałyby swoje wewnętrzne systemy identyfikowania, powiadamiania i reagowania na incydenty informacyjne.

2. Przygotowanie banków do odpowiedzi na sektorowy atak informacyjny. Banki określają role i zakresy odpowiedzialności zarówno wewnątrz poszczególnych instytucji, jak i w ramach wspólnej platformy wymiany informacji. Opracowywane są scenariusze potencjalnych ataków informacyjnych wraz z oceną ich prawdopodobieństwa oraz siły oddziaływania na banki i sektor. Na tej podstawie przygotowuje się strategie odpowiedzi na poziomie indywidualnym oraz sektorowym, a ZBP koordynuje współpracę banków w zakresie uzgodnienia podejścia, kanałów komunikacji oraz szablonów działań.

3. Prowadzenie cyklicznych ćwiczeń sektorowych. Realizowane są regularne ćwiczenia obejmujące odpowiedź na symulowane ataki informacyjne. ZBP planuje i koordynuje przebieg ćwiczeń, a banki testują szybkość i adekwatność działań podejmowanych w ramach ekosystemu reagowania. Wnioski z ćwiczeń stanowią podstawę aktualizacji dokumentów i standardów, a także doskonalenia oraz ewentualnej przebudowy ekosystemu reagowania na ataki informacyjne.

Tryb kryzysowy obejmuje następujące elementy:

1. Detekcja i klasyfikacja incydentu. Po wykryciu incydentu informacyjnego bank przekazuje informacje do ekosystemu reagowania na ataki informacyjne oraz inicjuje jego obsługę w trybie kryzysowym. Następuje identyfikacja kanałów dystrybucji, grup odbiorców, tematu oraz potencjalnych celów ataku informacyjnego. Równolegle dokonywana jest ocena ryzyka transmisji incydentu na inne banki oraz, w przypadku scenariuszy transgranicznych, na europejski system bankowy. ZBP uruchamia koordynację działań sektorowych adekwatnie do skali i dynamiki incydentu.

2. Wypracowanie sektorowego obrazu sytuacji oraz przekazu do mediów. Na podstawie wstępnej klasyfikacji incydentu uruchamiana jest wcześniej przygotowana strategia reagowania, a działania kryzysowe są dostosowywane do specyfiki zdarzenia. Banki aktywują kanały komunikacji zewnętrznej i wewnętrznej, w tym kanały obsługi zapytań klientów. W przypadku przeciążenia infolinii wdrażane są rozwiązania awaryjne, w szczególności komunikaty automatyczne przekierowujące klientów do innych kanałów kontaktu lub do oficjalnych, aktualizowanych źródeł informacji. W razie potrzeby działania te mogą być prowadzone we współpracy z operatorami telekomunikacyjnymi.

3. Wybór strategii odpowiedzi. W zależności od zasięgu oraz dotkliwości incydentu określa się poziom reakcji, na przykład brak reakcji, reakcja ograniczona do wybranych interesariuszy, reakcja sektorowa lub reakcja wymagająca koordynacji na poziomie krajowym i europejskim, w tym powiadomienia KNF. Dobierane są kanały komunikacji, a w przypadku incydentów o istotnym wpływie publikowany jest skoordynowany przekaz realizowany równolegle przez wiele banków, różnymi kanałami, niezależnie od kanału, w którym pierwotnie wystąpił atak informacyjny. W uzasadnionych przypadkach do komunikacji włącza się NBP w celu wzmocnienia wiarygodności przekazu.

4. Monitorowanie skutków incydentu i działania prowadzące do jego wygaszenia. Prowadzony jest bieżący monitoring przekazów medialnych oraz reakcji klientów i innych interesariuszy. Równolegle mierzona jest skuteczność dotychczasowej komunikacji, a komunikaty są aktualizowane wraz ze zmianą sytuacji informacyjnej. Po wygaszeniu incydentu przeprowadza się analizę wniosków i aktualizuje standardy, strategie, elementy ekosystemu reagowania, a także plany oraz zakres ćwiczeń sektorowych.

4.4. Rekomendacje dla polskiego sektora bankowego

W kontekście zawartości części czwartej można pokusić się o sformułowanie kilku rekomendacji pod adresem polskich banków, jak i regulatorów oraz władz. W odniesieniu do instytucji bankowych zasadne wydają się następujące działania:

- **Dywersyfikacja i redundancja infrastruktury krytycznej** – banki powinny geograficznie rozproszyć centra danych i systemy backupowe poza region potencjalnych konfliktów. Kluczowe jest posiadanie redundantnych systemów w lokalizacjach zachodnich (np. Frankfurt, Londyn) oraz zabezpieczenie łączności poprzez alternatywne kanały komunikacji; warto także wykorzystać rozwiązania chmurowe.
- **Działania na rzecz bezpiecznego i niezakłóconego dostępu do gotówki** – wypracowanie planów zarządzania zwiększonym popytem na gotówkę w kryzysie; zabezpieczanie fizycznych łańcuchów dostaw i przechowywani znaków pieniężnych; współpraca z NBP z bankami, firmami transportującymi i zabezpieczającymi gotówkę; wyważenie przez banki efektywności redukcji infrastruktury gotówkowej z względami stabilności systemu; działalność edukacyjna podnosząca świadomość znaczenia gotówki w sytuacjach kryzysowych.
- **Zróżnicowane bufory płynnościowe i rezerwy** – utrzymywanie rezerw nie tylko w PLN i EUR/USD, ale także w walutach i aktywach, które można traktować jako *safe havens* (CHF, JPY, ale i złoto, zwłaszcza w kontekście możliwości, jakie daje w tym zakresie Basel III oraz potencjalnego Bretton Woods III).
- **Konsekwentna implementacja zapisów DORA, MiCA i NIS2** – regulacje te powinny być postrzegane jako fundament odporności; należy jednak unikać tzw. *gold-plating*, mogącego stanowić tzw. *overkill* dla odporności systemowej na ryzyko geopolityczne.
- **Dbałość o suwerenność i bezpieczeństwo technologiczne** – ograniczanie zależności od dostawców z krajów potencjalnie wrogich lub niestabilnych; preferowanie rozwiązań europejskich lub z krajów sojuszniczych, zwłaszcza w infrastrukturze krytycznej.
- **Sektorowa analiza wrażliwości** – identyfikacja (na bazie ciągłej) branż szczególnie narażonych na konkretne ryzyka geopolityczne (energetyka, transport, przemysł zależny od importu surowców z Rosji/Chin). Różnicowanie wymogów kapitałowych i limitów koncentracji.
- Transparentna komunikacja z klientami – przygotowanie komunikatów kryzysowych wyjaśniających potencjalne ograniczenia w dostępie do usług, zamrożenia transakcji w przypadku sankcji, procedury ochrony depozytów; dbałość o przejrzystość decyzji i reputację. Wdrożenie sektorowego protokołu reagowania na atak informacyjny.
- Ryzyko geopolityczne jest w obecnych uwarunkowaniach centralną kwestią strategiczną dla polskich instytucji finansowych. Wymaga to stworzenia specjalnych struktur. Warto rozważyć **utworzenie w bankach (przynajmniej w tych szczególnie narażonych na ryzyko geopolityczne) stanowiska *Chief Geopolitical Risk Officer***. Osoba taka byłaby odpowiedzialna za integrację informacji geopolitycznych i działań w tym zakresie ze strategicznymi decyzjami i działaniami banku w określonych obszarach.

4.5. Rekomendacje pod adresem regulatorów i polityki gospodarczej

W odniesieniu do ogólnych ram funkcjonowania sektora bankowego można sformułować następujące rekomendacje dla regulatorów (Parlament, KNF) i decydentów (w szczególności ministerstw: finansów i gospodarki, obrony narodowej, funduszy i polityki regionalnej) w zakresie ograniczania ryzyka geopolitycznego:

- **Stworzenie kompleksowego modelu długotrwałej współpracy** między 4 grupami podmiotów (rząd, przedsiębiorstwa prywatne i państwowe z sektora obronnego, banki komercyjne (państwowe i prywatne) i ZBP, KNF). Celem tych działań ma być wsparcie bezpieczeństwa narodowego i rozwój polskiego sektora obronnego, gdyż niezbędne jest wykorzystanie – poprzez krajowy system bankowy – kapitału prywatnego do modernizacji tego sektora. Rząd reprezentowany powinien być przez ministerstwa: finansów, obrony narodowej, funduszy i polityki regionalnej.
- **Regularne spotkania merytoryczne** dot. współpracy między tymi podmiotami organizowane przez ministerstwa.

- **Wprowadzenie programu dot. zabezpieczenia finansowania długoterminowych inwestycji** poprzez KUKE albo BGK, w celu ograniczenia ekspozycji banku na klienta lub na dany projekt (projekty w sektorze zbrojeniowym są długoterminowe i wymagają wielkiego finansowego zaangażowania).
- **Wprowadzenie gwarancji** (KUKE, BGK, rząd) na zawarte kontrakty zbrojeniowe z zagranicą, co chroni producentów przed ryzykiem braku płatności od zagranicznych klientów (to jest ważne dla przedsiębiorstw, ich płynności finansowej i spłaty rat kredytów).
- **Ustalenie zasad raportowania banków do KNF** w przypadku finansowania projektów inwestycyjnych przedsiębiorstw z sektora zbrojeniowego objętych klauzulą informacji niejawnych.
- **Zapewnienie długoterminowości kontraktów** na zakup sprzętu od polskich przedsiębiorstw przez Skarb Państwa, tak aby zabezpieczyć zyskowność inwestycji i terminową spłatę kredytów.
- **Stworzenie systemowego wsparcia** (specjalne programy oferowane przez BGK, PFR) dotyczących finansowania, zabezpieczenia kredytów banków udzielanych startupom z sektora MŚP, które inwestują w projektowanie i produkcję innowacyjnych produktów *dual-use*.
- **Obniżenie istniejących ciężarów fiskalnych**, w tym rozważenie (trwałej lub czasowej) obniżki podatku CIT dla banków w okresach wysokiej ekspozycji na ryzyko geopolityczne, a także w okresach wzmożonego uczestnictwa w finansowaniu wydatków związanych z obronnością.
- **Dodatkowe gwarancje** dla instytucji bankowych zaangażowanych aktywnie w finansowanie zbrojeń oraz inwestycji energetycznych.
- **Zaoferowanie przez banki rachunków oszczędnościowo-inwestycyjnych** dla konsumentów, wsparte ulgami podatkowymi przez państwo, aby zachęcić do inwestowania i rozwijać krajowy rynek kapitałowy.
- **Rozważenie przez rząd i KNF zmniejszenia ograniczeń w rozwoju zdolności banków do akumulacji kapitału** (co ogranicza ich możliwości udzielenia kredytów) związanych z regulacjami i obecną konstrukcją podatku bankowego.
- **Rozważenie zmian w regulacjach** (ustawowy, KNF) dotyczących limitów zaangażowania banku/konsorcjum banków w dany projekt z sektora obronnego, z ekspozycją na Skarb Państwa (nowe rozwiązania np. w ustawie o obronie Ojczyzny, dodatkowe gwarancje ze strony państwa w przypadku przekroczenia limitów).

Uwagi końcowe

Ryzyko geopolityczne jest nieodłączną cechą współczesnego życia politycznego, gospodarczego i społecznego. Można uznać, że bezpieczne i sprzyjające wymianie handlowej i niezakłóconemu przepływowi kapitałów, osób i towarów warunki globalizacji oraz świata jednobiegunowego należą do przeszłości. Obserwujemy próby zorganizowania na nowo porządku światowego, dostosowanego do rzeczywistego, bieżącego potencjału poszczególnych państw i regionów, a także uwzględniającego warunki rewolucji technologicznej, tendencji demograficznych oraz zagrożeń i szans, przed jakimi stoi ludzkość jako gatunek (kwestie klimatyczne, eksploracja kosmosu, sztuczna inteligencja).

Ważną sferą rywalizacji geopolitycznej są systemy monetarne i finansowe (w tym bankowe). Powszechnym zjawiskiem jest tzw. weaponizacja walut, wojny walutowe, a systemy bankowe stanowią ważne ogniwo budowania przewagi konkurencyjnej przez poszczególne państwa, a jednocześnie (właśnie wskutek tego) są szczególnie narażone na atak ze strony państw wrogich lub konkurujących.

Polski system bankowy można uznać za stabilny i w dobrej kondycji. Niemniej pewne jego cechy (m.in. bardzo wysoki udział papierów dłużnych w portfelach, obciążenia fiskalne i ich konstrukcja) zwiększają jego podatność na realizację ryzyka geopolitycznego w jego rozmaitych wymiarach i aspektach.

Ryzyko geopolityczne w przeważającej mierze ma charakter egzogeniczny względem systemu bankowego. Jest też trudne do prognozowania i nie poddaje się *hedgingowi*. Z tych względów, możliwości samych banków zabezpieczania się przed tym ryzykiem są z natury rzeczy ograniczone. W pierwszej kolejności kluczowe są tu zatem działania na szczeblu całego państwa (decyzje polityczne, udział w międzynarodowych organizacjach i instytucjach, polityka makroekonomiczna, polityki sektorowe), a także koordynacja działań poszczególnych organów, instytucji i decydentów.

Z uwagi na trwające gwałtowne zmiany technologiczne, jednym z węzłowych obszarów w kontekście ryzyka geopolitycznego są obecnie kwestie dotyczące cyberbezpieczeństwa, cyberataków, odpowiedniego uregulowania cyfrowych aktywów (w tym zwłaszcza kryptowalut), zapewnienia redundancji systemów. Warto wskazać, że polski system bankowy można uznać za jeden z najbardziej innowacyjnych pod względem technologicznym, co najmniej w regionie.

Zapewnienie trwałej i większej odporności na ryzyko geopolityczne wymaga zrozumienia i odpowiedniego wyważenia (systemowych, długofalowych) korzyści płynących z jego zapewnienia z koniecznością ponoszenia (indywidualnych, krótkookresowych) kosztów w tym zakresie przez poszczególne instytucje bankowe. Wdrożenie sformułowanych w raporcie rekomendacji przez wszystkich interesariuszy powinno znacząco podnieść odporność systemu bankowego na ryzyko geopolityczne. Takie działania ze strony banków jak dywersyfikacja i redundancja infrastruktury krytycznej, działania na rzecz bezpiecznego i niezakłóconego dostępu do gotówki utrzymywanie zróżnicowanych buforów płynnościowych i rezerw, konsekwentna implementacja zapisów DORA, MiCA i NIS2, dbałość o suwerenność i bezpieczeństwo technologiczne, sektorowa analiza wrażliwości, transparentna komunikacja z klientami, czy wreszcie utworzenie w bankach stanowiska Chief Geopolitical Risk Officer, wsparte działaniami banku centralnego, nadzorców oraz organów rządowych pozwoliłoby z większym spokojem obserwować kształtowanie się ryzyka geopolitycznego. Tym bardziej, że najbliższym czasie trudno oczekiwać, by czynnik ten stracił na znaczeniu.

Aneks Przykładowe realizacje ryzyka geopolitycznego i ich konsekwencje dla polskiego systemu bankowego– scenariusze zdarzeń

Założenia

W niniejszym aneksie zawarto przykładowe, czysto hipotetyczne (aczkolwiek potencjalnie możliwe) scenariusze manifestacji ryzyka geopolitycznego, których wystąpienie może dotknąć polski system bankowy. Autorzy nie podejmują się szacowania prawdopodobieństwa wystąpienia poszczególnych scenariuszy, ani też ustalenia jakiejkolwiek hierarchii ich ważności. Poszczególne scenariusze można potraktować jako punkt wyjściowy do przeprowadzenia określonych stress testów. Rozpatrując poszczególne scenariusze, uwypuklono w nich te kanały transmisji ryzyka geopolitycznego, które uznano za szczególnie ważne z punktu widzenia przebiegu wydarzeń w danym scenariuszu. Wybierając poszczególne scenariusze, kierowano się obserwacją istniejących konfliktów i głównych punktów zapalnych, a także obszarów szczególnie wrażliwych z uwagi na uwarunkowania ryzyka geopolitycznego, które można odnieść, bezpośrednio lub pośrednio do gospodarki polskiej.

Z każdym scenariuszem wiążą się określone parametry: (1) główny kanał/y przenoszenia się ryzyka geopolitycznego; (2) horyzont czasowy – czas, w jakim manifestuje się dane ryzyko; oraz (3) ogólny wpływ na polski system bankowy – wyrażony jako jedna z trzech opcji: wariant umiarkowany, poważny oraz krytyczny. W odniesieniu do każdego scenariusza przedstawiono w pierwszej kolejności uzasadnienie jego rozważania, następnie przebieg wydarzeń (łącznie z charakterystyką wyzwalacza (triggera) w danym scenariuszu), główne kanały transmisji ryzyka geopolitycznego w scenariuszu, by wreszcie scharakteryzować syntetycznie wybrane potencjalne następstwa realizacji określonego scenariusza.

Na podstawie poszczególnych scenariuszy sporządzono następnie zbiorczą tabelę zawierającą ich główne charakterystyki. Ponadto w tabeli podjęto próbę określenia wpływu każdego scenariusza na główne rodzaje ryzyka bankowego: płynności, kredytowe, operacyjne oraz kapitałowe. Określając skalę tego wpływu, kierowano się czterema skalami ryzyka, które ujęto w tabeli 1.

Lista scenariuszy

1. **Eskalacja wojny na Ukrainie**
2. **Wycofanie się USA z Europy**
3. **Kryzys i fragmentacja Unii Europejskiej**
4. **Cyfrowe euro – fiasko implementacji**
5. **Waluta BRICS – The Unit (dekompozycja systemu walutowego)**
6. **Cyberatak na krajową infrastrukturę płatniczą**
7. **Cyberatak na infrastrukturę IT USA**
8. **Kryzys zaufania do AI w sektorze finansowym**
9. **Kryzys energetyczny 2.0 – permanentna drożyzna energii**
10. **Dezintegracja łańcuchów dostaw – nowy protekcjonizm**
11. **Eskalacja konfliktu wokół Tajwanu z szokiem podażowym**
12. **Perfect Storm (kumulacja negatywnych zdarzeń/wyzwalaczy ryzyka geopolitycznego)**

SCENARIUSZ 1 Eskalacja wojny na Ukrainie

Kanał dominujący	Horyzont	Wpływ ogólny
makro + płynnościowy + operacyjny	natychmiast	krytyczny

1. Uzasadnienie wystąpienia scenariusza

- Wojna na Ukrainie weszła w fazę przewlekłą, ale równowaga militarna jest krucha – każda zmiana wsparcia zachodniego lub wyczerpanie rezerw ludzkich może gwałtownie zmienić dynamikę konfliktu.
- Nasilenie działań możliwe wskutek determinacji strony rosyjskiej, nie odnoszącej spodziewanych sukcesów
- Eskalacja nie musi oznaczać ataku na Polskę – wystarczy rozszerzenie strefy działań (uderzenia na infrastrukturę poza Ukrainą, użycie broni niekonwencjonalnej), by wywołać systemową reakcję rynków.
- Polska, jako logistyczny hub dla dostaw na Ukrainę, goszczący największą liczbę ukraińskich uchodźców w Europie i wydający ponad 4% PKB na obronność, jest już głęboko uwikłana; eskalacja konfliktu dodatkowo zwiększy ekspozycję naszego kraju.
- Rosja dysponuje motywacją i zdolnościami do działań hybrydowych wymierzonych w polski system finansowy jako element infrastruktury krytycznej NATO.

2. Scenariusz – przebieg wydarzeń

- Przełom na linii frontu lub decyzja o bezpośrednim zaangażowaniu sił NATO zmienia charakter konfliktu z regionalnego na europejski – rynki finansowe reagują błyskawiczną przeceną aktywów krajów „flankowych".
- Polska ogłasza pełną mobilizację gospodarczo-militarną: wydatki obronne skaczą do 5–6% PKB, ogłaszane są kontrole przepływu kapitału i ograniczenia dewizowe.
- Uchodźcy z Ukrainy (kilka milionów osób) i potencjalna fala uchodźców z zachodniej Ukrainy generują nagłe obciążenia fiskalne i socjalne.
- Ataki hybrydowe (cyber, dezinformacja, sabotaż infrastruktury) na Polskę eskalują – system bankowy jako cel strategiczny.
- Złoty pod ekstremalną presją; NBP interweniuje na rynku FX, rozważa kontrolę przepływów kapitałowych.

3. Główne kanały transmisji i skutki dla banków

- **Kanał płynnościowy:** masowy odpływ kapitału zagranicznego; możliwy run na depozyty; możliwe uruchomienie gwarancji rządowych ponad limit BFG.
- **Kanał ryzyka kredytowego:** gwałtowne spowolnienie gospodarcze lub recesja – skokowy wzrost NPL we wszystkich segmentach portfela; deprecjacja złotego uderza w kredytobiorców z ekspozycją walutową; spadek wartości portfela obligacji skarbowych (wzrost *spreadów*).
- **Kanał operacyjny:** cyberataki na systemy bankowe – możliwe wielodniowe zakłócenia operacyjne; mobilizacja i pobór pozbawiają banki kluczowych pracowników IT i operacyjnych; koszty relokacji oddziałów z regionów zagrożonych.
- **Kanał makroekonomiczny:** nadzwyczajne podatki wojenne, przymusowe pożyczki dla budżetu; możliwe zawieszenie standardowych wymogów kapitałowych analogicznie do COVID-19.

4. Łączne potencjalne następstwa

- Pełne „upaństwowienie" ryzyka: granica między ryzykiem bankowym a ryzykiem kraju zaciera się; banki stają się ramieniem finansowym państwa w trybie wojennym.
- Trwałe przemodelowanie zarządzania ryzykiem: konieczność włączenia scenariuszy militarnych do standardowych stress-testów i planów ciągłości działania.
- Wzrost (skokowy) zapotrzebowania na gotówkę.
- Trwały odpływ kapitału zagranicznego: premia za ryzyko geopolityczne wbudowana w koszt kapitału polskich banków pozostaje trwale podwyższona nawet po zakończeniu kryzysu.

SCENARIUSZ 2 Wycofanie się USA z Europy

Kanał	Horyzont	Wpływ ogólny
rynkowy + makro + cyber	1–3 lata	poważny

1. Uzasadnienie wystąpienia scenariusza

- Tendencja „America First" ma charakter strukturalny, nie epizodyczny – USA stopniowo reorientują priorytet strategiczny na Indo-Pacyfik (tzw. *pivot* strategiczny).
- Zmęczenie wyborców amerykańskich kosztami obecności wojskowej w Europie tworzy trwałą bazę polityczną dla izolacjonizmu.
- Zaangażowanie USA w innych regionach (Iran); problemy budżetowe (presja na cięcie wydatków wojskowych za granicą).
- Europejczycy nie są w stanie szybko wypełnić luki bezpieczeństwa: brak wspólnej armii UE, niskie wydatki obronne większości krajów.
- Polska jako kraj flankowy NATO jest nieproporcjonalnie narażona – scenariusz rezygnacji USA uderza w Polskę mocniej niż w Europę Zachodnią.
- Wycofanie się USA nie musi być formalne – wystarczy sygnalizowanie warunkowego zaangażowania, by rynki wyceniły wzrost ryzyka.

2. Scenariusz – przebieg wydarzeń

- Administracja USA ogłasza redukcję kontyngentu wojskowego i rewizję zobowiązań NATO w ramach Artykułu 5; rynki interpretują to jako poważne ograniczenie gwarancji.
- Polska i kraje bałtyckie wchodzą w tryb defensywny: gwałtownie rosną wydatki obronne, pojawia się debata o własnych zdolnościach nuklearnych.
- Kapitał zagraniczny zaczyna wyceniać Polskę jako kraj podwyższonego ryzyka – odpływ inwestycji portfelowych, wzrost *spreadów* CDS na polskim długu.
- Złoty deprecjonuje gwałtownie; NBP staje przed wyborem między ochroną kursu a polityką wzrostu.
- Rosja odczytuje komunikaty/sygnały USA jako zielone światło dla działań hybrydowych w regionie.

3. Główne kanały transmisji i skutki dla banków

- **Kanał rynkowy:** gwałtowna deprecjacja złotego generuje straty kursowe i podnosi koszty finansowania zagranicznego.
- **Kanał kredytowy:** masowy wzrost wydatków obronnych przy ograniczonej przestrzeni fiskalnej – ryzyko podniesienia podatków; pogorszenie koniunktury i wzrost NPL.
- **Kanał płynnościowy:** masowy odpływ depozytów zagranicznych i inwestycji portfelowych osłabia bazę finansowania banków; możliwy run na banki.
- **Kanał operacyjny i cybernetyczny:** wycofanie wsparcia wywiadowczego i cyberbezpieczeństwa USA; infrastruktura krytyczna sektora bankowego pod zwiększoną presją.

4. Łączne potencjalne następstwa

- Trwały wzrost premii za ryzyko geopolityczne wbudowanej w koszt kapitału polskich banków – pogorszenie konkurencyjności w europejskim benchmarkingu.
- Militaryzacja budżetu i jej efekty wypychające: gwałtowny wzrost wydatków obronnych ogranicza przestrzeń fiskalną i pośrednio obciąża banki przez kanał makro (kwestie fiskalne).
- Presja na polskie banki jako „pożyczkodawców ostatniej szansy" dla budżetu w sytuacji trudnego dostępu do rynków zewnętrznych.
- Paradoks bezpieczeństwa: próba budowy europejskiej autonomii strategicznej może krótkoterminowo pogłębiać niestabilność finansową.

SCENARIUSZ 3 Kryzys i fragmentacja Unii Europejskiej

Kanał	Horyzont	Wpływ ogólny
rynkowy + regulacyjny + makro	3–7 lat	poważny

1. Uzasadnienie wystąpienia scenariusza

- Narastające napięcia między „starą" a „nową" Europą w kwestiach praworządności, polityki migracyjnej i transferów fiskalnych osłabiają spoistość UE.
- Brak unii fiskalnej przy istniejącej unii monetarnej tworzy strukturalną asymetrię: w razie kryzysu i szoku asymetrycznego kraje mają sprzeczne interesy.
- Wzrost partii eurosceptycznych w kluczowych krajach (Francja, Niemcy, Włochy) otwiera scenariusze wyjścia z UE lub radykalnej renegocjacji traktatów.
- Rozszerzenie UE (Ukraina, Bałkany) przy braku reform instytucjonalnych grozi paraliżem decyzyjnym.
- Polska jako kraj silnie uzależniony od funduszy unijnych i dostępu do wspólnego rynku jest strukturalnie najbardziej narażona spośród krajów „nowej" UE
- Spory o pakiet klimatyczny i system ETS pogłębiają podziały Wschód-Zachód.
- Precedens: Brexit (2016–2020) pokazał, że kształt UE może zmienić się nie tylko wskutek rozszerzenia.

2. Scenariusz – przebieg wydarzeń

- Kryzys polityczny w którymś z głównych krajów UE: nowy rząd kwestionujący zobowiązania traktatowe; rynki reagują gwałtownym wzrostem *spreadów* obligacji skarbowych.
- EBC staje przed dylematem: interweniować lub nie interweniować – każda decyzja generuje polityczne konsekwencje.
- Niemcy blokują kolejny pakiet pomocowy; pojawia się debata o „twardym euro" dla krajów Północy.
- Polska traci dostęp do kolejnej transzy funduszy strukturalnych wskutek impasu budżetowego UE.
- Scenariusz nie musi oznaczać formalnego rozpadu UE – wystarczy trwały paraliż decyzyjny i erozja jednolitego rynku, by skutki dla Polski były poważne.
- **Scenariusz optymistyczny:** UE pozostaje jako unia celna, ale obszar euro rozpada się na 2–3 strefy; **scenariusz pesymistyczny:** Pełny rozpad UE.

3. Główne kanały transmisji i skutki dla banków

- **Kanał makroekonomiczny:** spowolnienie gospodarcze wskutek ograniczenia funduszy UE, osłabienia eksportu i spadku inwestycji – wzrost NPL w portfelach korporacyjnych i detalicznych; recesja i bezrobocie; bankructwa firm zorientowanych na jednolity rynek.
- **Kanał kredytowy:** wzrost NPL w odniesieniu do kredytów korporacyjnych (zwłaszcza eksporterów); wzrost NPL w odniesieniu do kredytów dla MŚP.
- **Kanał regulacyjny:** dezintegracja unijnej architektury nadzorczej (SSM, SRM) – KNF musi przejąć ciężar nadzoru bez europejskiego zaplecza; repatriacja kapitału zagranicznego, poszukiwania kapitału lokalnego (ale brak chętnych w kryzysie).
- **Kanał rynkowy:** wzrost zmienności i odpływ kapitału z polskiego rynku obligacji i akcji – presja na płynność i wyceny portfeli banków; deprecjacja złotego względem CHF.

4. Łączne potencjalne następstwa

- Repolonizacja sektora bankowego: państwo i krajowe podmioty przejmują udziały od wychodzących grup zagranicznych
- Wzrost kosztów finansowania państwa: słabszy parasol UE oznacza wyższe premie za ryzyko na polskim długu; banki jako główni nabywcy obligacji absorbują to ryzyko do bilansów.
- Konieczność redefinicji modelu biznesowego: banki opierające się na przepływach transgranicznych muszą przeprojektować struktury finansowania.
- Paradoks gotówki: erozja zaufania do europejskich instytucji może zwiększyć popyt na gotówkę jako środek skarbienia (tezauryzacji), mimo wzrostu skali rozliczeń bezgotówkowych.

SCENARIUSZ 4 Cyfrowe euro – fiasko implementacji

Kanał	Horyzont	Wpływ ogólny
zaufania i reputacji + łańcuchów dostaw i powiązań	3–7 lat	umiarkowany

1. Uzasadnienie wystąpienia scenariusza

- EBC jest obecnie (wiosna 2026) po etapie przygotowawczym, który trwał od listopada 2023 do października 2025; prowadzone są dalsze prace techniczne i legislacyjne. Jeśli w 2026 r. prawodawcy unijni przyjmą odpowiednie przepisy, emisja cyfrowego euro będzie zdaniem EBC możliwa w 2029 r.
- Projekt cyfrowego euro napotyka fundamentalne sprzeczności: EBC chce zachować stabilność sektora bankowego i jednocześnie stworzyć środek płatniczy konkurencyjny wobec depozytów bankowych.
- Wewnętrzne podziały w Radzie Prezesów EBC (oś Północ–Południe) prowadzą do niespójnych decyzji projektowych i wielokrotnych restartów projektu.
- Masowy opór polityczny – partie populistyczne i libertariańskie w całej UE mobilizują wyborców pod hasłem „pieniądza nadzoru".
- Problemy techniczne w fazie pilotażowej (bezpieczeństwo, brak funkcji offline, niska adopcja) podkopują zaufanie jeszcze przed właściwym wdrożeniem.
- Presja lobbingowa sektora bankowego i Fintech skutkuje kompromisami projektowymi – cyfrowe euro traci rację bytu w oczach użytkowników.
- Polska jako kraj spoza strefy euro obserwuje fiasko z zewnątrz, ale ponosi konsekwencje systemowe ze względu na głębokie powiązania ze strefą euro.
- **Precedensy fiaska:** (1) Libra/Diem (Meta): anulowana po 3 latach rozwoju (2019–2022); (2) E-krona (Szwecja): pilotaż od 2020 r., ciągle bez wdrożenia; (3) cyfrowy yuan (Chiny) – uruchomiony, ale przyjęcie (adopcja) poniżej 10%, mimo dużych nacisków politycznych.

2. Scenariusz – przebieg wydarzeń

- EBC ogłasza harmonogram wdrożenia, jednak z każdą rundą konsultacji projekt jest „okrawany" z kluczowych funkcji; ostateczny produkt nie spełnia oczekiwań ani banków, ani użytkowników.
- Uruchomienie (*launch*) techniczne odbywa się zgodnie z planem, jednak adopcja jest wielokrotnie niższa od prognoz.
- W ciągu pierwszych miesięcy dochodzi do incydentu bezpieczeństwa, który wywołuje europejską debatę o bezpieczeństwie infrastruktury cyfrowej EBC.
- Rządy kilku krajów strefy euro inicjują parlamentarne przesłuchania; w Parlamencie Europejskim formuje się blokująca koalicja.
- EBC oficjalnie „wstrzymuje" projekt na czas „przeglądu technicznego i regulacyjnego" – rynek odczytuje to jako de facto odwołanie.
- USA rezygnują z projektu cyfrowego dolara (zakaz CBDC obecnie do 2030 r.), a Chiny agresywnie promują e-CNY – geopolityczna próżnia w walutach cyfrowych zachodnich instytucji staje się faktem.

3. Główne kanały transmisji i skutki dla banków

- **Kanał zaufania i reputacji:** osłabienie wiarygodności EBC; polskie banki muszą przepisać strategie dostosowawcze – koszty „zmarnowanych" prac przygotowawczych.
- **Kanał łańcuchów dostaw i powiązań:** próżnię wypełniają prywatne rozwiązania – stablecoiny, platformy BigTech (Apple Pay, Google Pay) spoza jurysdykcji UE.
- **Kanał operacyjny:** banki, które poniosły nakłady na integrację z infrastrukturą cyfrowego euro, odpisują te inwestycje.
- **Kanał suwerenności i czynników politycznych:** złoty zyskuje na autonomii, ale traci parasol ochronny wspólnej architektury regulacyjnej.

4. Łączne potencjalne następstwa

- Utrata *momentum* modernizacyjnego: polska bankowość traci impuls do konwergencji z europejską infrastrukturą płatniczą nowej generacji.
- Fragmentacja ekosystemu płatniczego: zamiast jednego standardu europejskiego – mozaika rozwiązań prywatnych i nieeuropejskich; wyższe koszty operacyjne i *compliance*.
- Przesunięcie ryzyka systemowego: rośnie udział podmiotów niebankowych w krytycznej infrastrukturze płatniczej – nowe ryzyka trudno mierzalne tradycyjnymi narzędziami nadzorczymi.
- Efekt demonstracyjny dla CBDC: fiasko cyfrowego euro zniechęca do analogicznych projektów w Polsce na wiele lat; problem obniża też skłonność do przyjęcia w Polsce euro samego w sobie; debata o znaczeniu gotówki odżywa ze zdwojoną siłą.

SCENARIUSZ 5 Wprowadzenie wspólnej waluty BRICS (The Unit) – dekompozycja systemu walutowego

Kanał	Horyzont	Wpływ ogólny
rynkowy + operacyjny	5–10 lat	umiarkowany

1. Uzasadnienie wystąpienia scenariusza

- Projekt „The Unit" jest odpowiedzią na „weaponizację" dolara – użycie SWIFT jako narzędzia sankcji po 2022 r.; motywacja polityczna i strukturalna, nie koniunkturalna.
- Kraje BRICS+ kontrolują rosnący udział w globalnym PKB (PPP), handlu surowcami i rezerwach złota – mają zasoby, by taki projekt częściowo uprawomocnić.
- Dolaryzacja handlu surowcami stopniowo słabnie: ropa rozliczana w juanach, umowy bilateralne omijające SWIFT – The Unit byłby formalizacją istniejących trendów.
- Scenariusz nie zakłada zastąpienia dolara – wystarczy, że The Unit stanie się wiarygodną alternatywą dla finansowania 30–40% globalnego handlu, by zachwiać hegemonią dolara i euro.
- Polska jako gospodarka eksportowa silnie powiązana z globalnym łańcuchem dostaw odczuje skutki dekompozycji pośrednio, ale dotkliwie.

2. Scenariusz – przebieg wydarzeń

- Szczyt BRICS ogłasza uruchomienie The Unit jako instrumentu rozliczeniowego; wspólna waluta (środek płatniczy?) częściowo zabezpieczona złotem i koszykiem surowców.
- W pierwszej fazie The Unit funkcjonuje wyłącznie jako jednostka rozliczeniowa – handel ropą, gazem i metalami coraz częściej bez udziału dolara i euro.
- Kraje Globalnego Południa stopniowo dywersyfikują rezerwy walutowe – sprzedają dolary i euro, kupują złoto i aktywa denominowane w The Unit.
- System SWIFT traci monopol na rozliczenia; równolegle funkcjonuje infrastruktura CIPS i nowe platformy krajów BRICS bazujące na łańcuchu bloków.
- Polscy eksporterzy zaczynają rozliczać się w juanie lub The Unit z kontrahentami z BRICS – polskie banki muszą obsługiwać nowe waluty i systemy płatnicze.

3. Główne kanały transmisji i skutki dla banków

- **Kanał rynkowy:** osłabienie dolara i euro jako walut rezerwowych wymusza zmianę struktury rezerw NBP i banków komercyjnych; wzrost globalnych stóp procentowych (obrona pozycji dolara/euro) podnosi koszty finansowania hurtowego polskich banków.
- **Kanał operacyjny:** konieczność integracji z nowymi systemami (CIPS, platformy The Unit) – wysokie koszty technologiczne i prawne; ryzyko wtórnych sankcji zachodnich.
- **Kanał makroekonomiczny:** wzrost cen surowców importowanych – stagflacyjna presja na gospodarkę, wzrost NPL w sektorach energochłonnych.

4. Łączne potencjalne następstwa

- Strukturalne zwiększenie kosztów operacyjnych: obsługa dwóch równoległych ekosystemów walutowych i płatniczych jest trwale droższa.
- Konieczność redefinicji polityki kursowej NBP: w świecie multipolarnym złoty nie może być prostą pochodną euro.
- Nowe ryzyka *compliance*: polskie banki muszą budować kompetencje w zakresie regulacji dwóch bloków jednocześnie; ryzyko naruszenia sankcji zachodnich przy obsłudze handlu z BRICS.
- Paradoks dywersyfikacji: dekompozycja systemu może krótkoterminowo zaszkodzić polskim bankom, ale długoterminowo otworzyć nowe rynki i strumienie przychodów.

SCENARIUSZ 6 Cyberatak dużej skali na krajową infrastrukturę płatniczą

Kanał	Horyzont	Wpływ ogólny
cyberbezpieczeństwa + zaufania i reputacji + płynnościowy	natychmiast	krytyczny

1. Uzasadnienie wystąpienia scenariusza

- Polska infrastruktura płatnicza należy do najbardziej zaawansowanych cyfrowo w Europie – wysoki poziom bankowości elektronicznej, BLIK, płatności mobilne tworzą atrakcyjny cel i wysoką podatność jednocześnie.
- Polska jako kraj NATO na wschodniej flance jest priorytetowym celem rosyjskich i białoruskich operacji cybernetycznych – ataki na infrastrukturę krytyczną są udokumentowanym narzędziem presji hybrydowej.
- Koncentracja systemów rozliczeniowych (KIR, SORBNET2, Express Elixir) tworzy wąskie gardła: zaatakowanie kilku węzłów może sparaliżować cały system.
- Grupy APT powiązane z państwami działają w polskich sieciach od lat – atak może być uruchomiony w dowolnym momencie z wcześniej przygotowanych przyczółków.

2. Scenariusz – przebieg wydarzeń

- Skoordynowany atak (np. ransomware) na kilka elementów infrastruktury jednocześnie: KIR, SORBNET2, wybrane banki komercyjne i NBP.
- Pierwsze godziny: niemożność wykonywania przelewów, awarie bankowości elektronicznej i mobilnej, błędy w saldach – utrudniona komunikacja banków z klientami; blokada 70–80% transakcji elektronicznych w kraju; paraliż bankomatów i POS; run na banki, kolejki przed oddziałami.
- Media społecznościowe podsycają panikę – fałszywe informacje o utracie depozytów i upadłości banków.
- Dni 2–5: system działa fragmentarycznie; gotówka staje się jedynym sprawnym środkiem płatniczym, ale bankomaty mają ograniczone zasoby.
- Rząd ogłasza stan wyjątkowy dla infrastruktury krytycznej; śledztwo wskazuje na atak państwowy.

3. Główne kanały transmisji i skutki dla banków

- **Kanał cyberbezpieczeństwa – kanał fundamentalny w tym scenariuszu; poszczególne wydarzenia manifestują się najpierw właśnie tutaj.**
- **Kanał operacyjny:** niemożność realizacji rozliczeń międzybankowych – zamrożenie płynności w całym systemie; zakłócenia systemu SEPA blokują płatności transgraniczne; przejściowa niewydolność infrastruktury gotówkowej.
- **Kanał zaufania i reputacji:** panika klientów – próby masowego wypłacania gotówki; trwałe naruszenie zaufania do bankowości elektronicznej.
- **Kanał płynnościowy:** gwałtowny wzrost popytu na gotówkę; koszt awaryjnych dostaw gotówki przez NBP (druk w trybie nadzwyczajnym).
- **Kanał operacyjny:** koszty przywrócenia systemów, audytów bezpieczeństwa, odszkodowań dla klientów; ryzyko kar regulacyjnych za niewystarczające zabezpieczenia (DORA).

4. Łączne potencjalne następstwa

- Pogorszenie wyników banków.
- Strukturalne przemodelowanie wymogów bezpieczeństwa: nowe, znacznie bardziej rygorystyczne standardy odporności cybernetycznej jako trwały koszt prowadzenia działalności bankowej.
- Renesans gotówki i fizycznej infrastruktury: incydent stanowi najsilniejszy możliwy argument za utrzymaniem gotówki w obiegu; możliwe regulacyjne wymogi minimalnych zapasów gotówki w bankomatach; redundancja rozwiązań w zakresie zaopatrzenia w gotówkę.
- Konsolidacja jako odpowiedź na ryzyko: ekonomia skali w cyberbezpieczeństwie faworyzuje większe instytucje.
- Suwerenność technologiczna jako priorytet regulacyjny: presja na lokalizację krytycznych systemów IT na terytorium Polski i budowę zapasowych węzłów rozliczeniowych.

SCENARIUSZ 7 Rozległy cyberatak na infrastrukturę IT Stanów Zjednoczonych

Kanał	Horyzont	Wpływ ogólny
operacyjny + rynkowy + łańcuchów dostaw i powiązań	natychmiast	poważny

1. Uzasadnienie wystąpienia scenariusza

- USA są węzłem centralnym globalnej infrastruktury cyfrowej: dominujące chmury obliczeniowe (AWS, Azure, Google Cloud), globalne sieci CDN, kluczowe węzły BGP i DNS – atak na nie uderza w cały świat jednocześnie.
- Precedensy: SolarWinds (2020), Colonial Pipeline (2021) – każdy kolejny atak jest bardziej wyrafinowany; znaczące (i znane państwom-rywalom) „skumulowane" podatności.
- Motywacja Rosji, Chin, Iranu i Korei Północnej do przeprowadzenia paraliżującego uderzenia cybernetycznego rośnie w kontekście eskalacji napięć geopolitycznych.
- Polskie banki są głęboko uzależnione od infrastruktury IT zlokalizowanej w USA lub zarządzanej przez amerykańskie korporacje – przez chmury, VISA/Mastercard, systemy SWIFT z węzłami w USA.

2. Scenariusz – przebieg wydarzeń

- Skoordynowany atak na systemy finansowe (Fed, CHIPS), chmury obliczeniowe, węzły DNS i BGP wywołuje kaskadowe awarie globalne.
- Globalne systemy płatności kartowych (VISA, Mastercard) działają w trybie awaryjnym lub są niedostępne przez kilka–kilkanaście godzin; transakcje kartowe w Polsce zawieszone.
- Rynki finansowe w USA zawieszone; europejskie giełdy i rynki walutowe działają w chaosie informacyjnym – niemożność wyceny ryzyka w czasie rzeczywistym.
- Atakujący używają okna czasowego do wtórnych ataków na europejską infrastrukturę, korzystając z paraliżu służb skupionych na USA.

3. Główne kanały transmisji i skutki dla banków

- **Kanał operacyjny:** awaria usług chmurowych AWS/Azure/GCP paraliżuje systemy bankowe oparte na tych platformach; niedostępność SWIFT z węzłami w USA blokuje płatności transgraniczne; ryzyko kaskadowych awarii infrastruktury teleinformatycznej wykorzystywanej przez banki; ryzyko przejścia kluczowych procesów w tryb manualny.
- **Kanał rynkowy:** panika na globalnych rynkach finansowych przekłada się na gwałtowne ruchy kursowe – złoty pod ekstremalną presją deprecjacyjną.
- **Kanał zaufania i reputacji:** globalny kryzys zaufania do cyfrowej infrastruktury finansowej; presja dezinformacyjna na konkretne banki – ryzyko runu nawet na banki w dobrej kondycji; szum informacyjny sprzyjający atakom socjotechnicznym; możliwy odpływ części klientów do systemów kryptowalut przy dłuższych zakłóceniach kanałów płatniczych.
- **Kanał łańcuchów i powiązań:** USA uruchamiają protokoły wojenne dla infrastruktury finansowej – możliwe tymczasowe ograniczenia w przepływach kapitałowych i dostępie do systemu dolarowego.

4. Łączne potencjalne następstwa

- Przyspieszenie debaty o suwerenności cyfrowej: uzależnienie od infrastruktury IT w USA staje się kwestią bezpieczeństwa narodowego; presja regulacyjna na lokalizację danych i systemów krytycznych w Europie.
- Wzrost przezornościowego motywu popytu na pieniądz.
- Renesans lokalnych systemów płatniczych: BLIK jako jeden z niewielu sprawnych systemów podczas globalnego paraliżu staje się argumentem za rozwojem autonomicznych krajowych infrastruktur płatniczych.
- Skokowy wzrost kosztów operacyjnych.
- Trwała zmiana architektury IT banków: wymóg redundancji geograficznej, zakaz monokultur chmurowych, obowiązkowe lokalne kopie zapasowe krytycznych danych i systemów.
- Szansa: Polska z silną tradycją gotówkową i lokalnym BLIK może wyjść z kryzysu relatywnie lepiej niż kraje bardziej zależne od globalnej infrastruktury – o ile wcześniej zadba o odporność lokalnych systemów.

SCENARIUSZ 8 Kryzys zaufania do AI w sektorze finansowym

Kanał	Horyzont	Wpływ ogólny
operacyjny + regulacyjny + zaufania i reputacji	1–5 lat	poważny

1. Uzasadnienie wystąpienia scenariusza

- Sektor finansowy wdraża AI w tempie szybszym niż ramy regulacyjne i metodologie zarządzania ryzykiem są w stanie nadążyć – klasyczna luka między innowacją a nadzorem.
- Modele AI trenowane na tych samych zbiorach danych tworzą „systemową homogeniczność" decyzji: wszyscy widzą to samo ryzyko tak samo – i wszyscy mylą się jednocześnie.
- Koncentracja dostawców infrastruktury AI (kilka globalnych chmur, kilka firm dostarczających modele bazowe) tworzy nowe ryzyko operacyjne o charakterze systemowym.
- Wrogie państwa mogą celowo „zatruwać" dane treningowe lub atakować infrastrukturę AI, by wywołać systemowe błędy decyzyjne w zachodnim sektorze finansowym.

2. Scenariusz – przebieg wydarzeń

- Duży europejski bank lub instytucja zarządzająca aktywami ujawnia, że jego model AI przez kilka miesięcy działał wadliwie – generując systematycznie błędne decyzje niewidoczne dla ludzkiego nadzoru.
- Śledztwo regulacyjne ujawnia, że podobne modele stosuje kilkanaście innych instytucji – korelacja błędów jest wysoka, bo modele bazują na tych samych danych.
- Regulatorzy (EBA, krajowe nadzory) nakazują wstrzymanie automatycznych decyzji kredytowych – instytucje muszą w krótkim czasie wrócić do procesów manualnych.
- Ujawniane są dowody na celowe ataki na modele AI przez podmioty państwowe – scenariusz cybernetyczny nakłada się na technologiczny.

3. Główne kanały transmisji i skutki dla banków

- **Kanał operacyjny:** banki, które głęboko zastąpiły procesy manualne systemami AI, stają wobec niemożności obsługi normalnego wolumenu decyzji; koszty operacyjne gwałtownie rosną.
- **Kanał kredytowy:** portfele zbudowane przy pomocy wadliwych modeli wymagają gruntownego przeglądu; część kredytów błędnie wycenionych.
- **Kanał regulacyjny:** fala pozwów ze strony klientów; regulatorzy zaostrzają wymogi dotyczące *explainability* modeli AI i ludzkiego nadzoru.
- **Kanał zaufania i reputacji:** utrata zaufania do zautomatyzowanych procesów bankowych – wzrost popytu na obsługę przez człowieka, co koliduje z modelem kosztowym nowoczesnej bankowości.

4. Łączne potencjalne następstwa

- Trwała zmiana modelu zarządzania ryzykiem: powrót do wymogu human in the loop dla istotnych decyzji; wyższe koszty operacyjne jako trwały element modelu biznesowego.
- Nowa oś przewagi konkurencyjnej: banki, które zachowały kompetencje eksperckie i nie przeszły na w pełni automatyczne procesy, wychodzą z kryzysu silniejsze.
- Geopolityczny wymiar infrastruktury AI: presja na korzystanie z europejskich lub krajowych dostawców AI zamiast globalnych platform.
- Wzrost wartości danych własnych i unikalnych: instytucje z poufnymi, zastrzeżonymi danymi i własnymi modelami okazują się mniej podatne na systemowe błędy wynikające z homogeniczności.

SCENARIUSZ 9 Kryzys energetyczny 2.0 – permanentna drożyzna energii

Kanał	Horyzont	Wpływ ogólny
kredytowy + makro	trwały	poważny

1. Uzasadnienie wystąpienia scenariusza

- Paradoks transformacji energetycznej: presja regulacyjna (Fit for 55, taksonomia UE) ogranicza inwestycje w paliwa kopalne szybciej niż OZE są w stanie wypełnić lukę.
- Niedoinwestowanie w wydobycie ropy i gazu przez dekadę (ESG, regulacje) tworzy trwałą premię cenową niezależną od bieżącej koniunktury.
- Geopolityka wzmacnia efekt: odcięcie od rosyjskich surowców jest trwałe (?), alternatywne źródła (LNG) są droższe i mniej stabilne.
- Polska jest szczególnie narażona: wysoka energochłonność przemysłu, duży udział węgla w miksie energetycznym, ekspozycja na ceny CO_2 w systemie ETS, niska efektywność energetyczna zasobu mieszkaniowego.
- Scenariusz zakłada trwałe ukształtowanie się cen energii na poziomie wielokrotnie wyższym niż historyczne średnie; zmienia to rachunek rentowności całych sektorów.

2. Scenariusz – przebieg wydarzeń

- Kolejna zima z niedoborami gazu lub ropa powracająca do historycznych szczytów – tym razem bez perspektywy rychłego powrotu do niskich cen.
- Rząd polski wprowadza kolejne rundy osłon energetycznych – rosnący deficyt budżetowy, presja na dług publiczny.
- Firmy energochłonne (hutnictwo, chemia, ceramika, przetwórstwo) tracą konkurencyjność; część przenosi produkcję poza UE lub zawiesza działalność.
- Koszty utrzymania mieszkań rosną nieproporcjonalnie do wynagrodzeń – gospodarstwa domowe mają trudności z obsługą kredytów.
- NBP stoi przed dylematem stagflacyjnym: wysoka inflacja wymaga wysokich stóp procentowych, ale recesja przemysłowa wymaga ich obniżek.

3. Główne kanały transmisji i skutki dla banków

- **Kanał operacyjny:** bezpośrednie konsekwencje wyższych cen energii dla instytucji bankowych – wzrost kosztów funkcjonowania.
- **Kanał kredytowy:** wzrost NPL w sektorach energochłonnych – hutnictwo, chemia, transport, rolnictwo; część przedsiębiorców traci rentowność trwale, nie przejściowo; wzrost kosztów utrzymania ogranicza zdolność klientów detalicznych do obsługi kredytów hipotecznych i konsumpcyjnych; nieruchomości o niskiej efektywności energetycznej tracą wartość jako zabezpieczenie.
- **Kanał makroekonomiczny:** stagflacja ogranicza przestrzeń manewru NBP; rosnący dług publiczny podnosi premię za ryzyko na polskich obligacjach skarbowych.

4. Łączne potencjalne następstwa

- Trwałe pogorszenie jakości portfeli kredytowych w sektorach przemysłowych – konieczność budowania wyższych rezerw przez wiele lat.
- Redefinicja polityki kredytowej: banki zmuszone do wbudowania ryzyka energetycznego w standardowe modele scoringowe i wyceny zabezpieczeń.
- Wzrost znaczenia „zielonego" finansowania: banki, które wcześniej zbudują kompetencje w finansowaniu OZE i efektywności energetycznej, zyskują przewagę konkurencyjną.
- Gotówka i fizyczna infrastruktura płatnicza zyskują na znaczeniu w scenariuszu przerw w dostawach energii.

SCENARIUSZ 10 Dezintegracja łańcuchów dostaw – nowy protekcjonizm

Kanał	Horyzont	Wpływ ogólny
kredytowy + powiązań i łańcuchów dostaw	trwały	poważny

1. Uzasadnienie wystąpienia scenariusza

- Globalizacja weszła w fazę odwrotu: *friendshoring*, *reshoring*, *nearshoring* jako wyraźne trendy w przepływach BIZ i lokalizacji produkcji.
- Wojny celne USA–Chiny, unijne mechanizmy ochrony rynku (CBAM) i amerykańskie ustawy przemysłowe (IRA, CHIPS Act) tworzą systemową presję na fragmentację globalnych łańcuchów wartości.
- Polska jest jednym z głównych beneficjentów dotychczasowej globalizacji w Europie – hub produkcyjny dla motoryzacji, elektroniki, AGD, logistyki; utrata tej roli byłaby szokiem strukturalnym.
- Scenariusz pozornie niegroźny, z czasem ujawnia się poważne zagrożenie: nie pojawia się jako jednorazowy kryzys, lecz jako powolna erozja pozycji konkurencyjnej, trudna do uchwycenia w klasycznych modelach ryzyka bankowego.

2. Scenariusz – przebieg wydarzeń

- USA nakładają kolejne cła na produkty europejskie; UE odpowiada środkami ochronnymi wobec Chin – spirala protekcjonistyczna ogranicza globalny handel.
- Europejski sektor motoryzacyjny restrukturyzuje łańcuchy dostaw – część produkcji wraca do Niemiec lub przenosi się poza UE; polskie zakłady tracą zamówienia.
- Chiny przestają być „fabryką świata" dla elektroniki – alternatywne lokalizacje (Indie, Wietnam, Meksyk) wygrywają z Polską w przetargach o nowe inwestycje.
- Polskie firmy MŚP głęboko wbudowane w łańcuchy dostaw korporacji tracą kontrakty bez możliwości szybkiego przestawienia się na nowych odbiorców.

3. Główne kanały transmisji i skutki dla banków

- **Kanał kredytowy:** stopniowy, trwały wzrost NPL w portfelach obsługujących sektor produkcyjny, logistyczny i motoryzacyjny; zamykanie zakładów produkcyjnych i centrów logistycznych uderza w rynek nieruchomości przemysłowych – deprecjacja zabezpieczeń w portfelach kredytowych; wzrost bezrobocia w regionach przemysłowych przekłada się na wzrost NPL w portfelach hipotecznych i konsumpcyjnych.
- **Kanał makroekonomiczny:** recesja, stagflacja, znaczące bezrobocie i strukturalne problemy gospodarki; spadającą międzynarodowa konkurencyjność gospodarki polskiej, niepewne miejsce w nowym światowym podziale pracy.

4. Łączne potencjalne następstwa

- Strukturalna zmiana profilu ryzyka sektora bankowego: od portfela zdywersyfikowanego ku portfelowi skoncentrowanemu na usługach i budownictwie krajowym.
- Regionalizacja ryzyka bankowego: problemy skupione w konkretnych regionach przemysłowych – potrzeba tzw. „granularnego" zarządzania ryzykiem geograficznym.

- Paradoks *nearshoringu*: część relokacji może przynieść Polsce nowe inwestycje (*reshoring* z Azji); banki z kompetencjami w nowych sektorach (zielona energia, obronność) mogą na tym zyskać.
- Wzmocnienie roli państwa jako inwestora i gwaranta kredytowego – BGK i fundusze gwarancyjne jako substytut kurczących się BIZ.

SCENARIUSZ 11 Eskalacja konfliktu wokół Tajwanu z szokiem podażowym

Kanał	Horyzont	Wpływ ogólny
rynkowy + kredytowy + makro	3–7 lat	krytyczny

1. Uzasadnienie wystąpienia scenariusza

- Tajwan produkuje ponad 90% najbardziej zaawansowanych mikroprocesorów na świecie (TSMC) – żadna inna lokalizacja nie jest w stanie szybko zastąpić tej zdolności produkcyjnej.
- Napięcie wokół Tajwanu narasta cyklicznie i ma charakter strukturalny: dla Chin zjednoczenie jest kwestią legitymizacji i prestiżu, dla USA i Tajwanu – przetrwania strategicznego.
- Blokada morska lub atak na Tajwan wywołałby natychmiastowy globalny szok podażowy w półprzewodnikach, porównywalny do szoku naftowego lat 70. – z tą różnicą, że półprzewodniki przenikają do każdego sektora nowoczesnej gospodarki.
- Polska jest narażona pośrednio, ale silnie: przez łańcuchy dostaw przemysłowych i przez globalny szok finansowy.

2. Scenariusz – przebieg wydarzeń

- Chiny ogłaszają blokadę morską Tajwanu; USA i sojusznicy wprowadzają sankcje o bezprecedensowej skali; dostawy mikroprocesorów zostają wstrzymane.
- Globalny rynek finansowy reaguje gwałtowną przeceną aktywów ryzykownych – *risk-off* na skalę przekraczającą kryzys 2008; kapitał ucieka do dolara, jena i złota.
- Łańcuchy dostaw dla europejskiego przemysłu (motoryzacja, elektronika, sprzęt medyczny, telekomunikacja) ulegają przerwaniu; fabryki redukują lub zawieszają produkcję z powodu braku podzespołów.
- Polska gospodarka wchodzi w głęboką recesję przemysłową: zakłady produkcyjne wstrzymują działalność, eksport gwałtownie spada, bezrobocie rośnie.

3. Główne kanały transmisji i skutki dla banków

- **Kanał kredytowy:** gwałtowny wzrost NPL w sektorach zależnych od półprzewodników – motoryzacja, elektronika, AGD, logistyka; to znaczna część portfeli kredytowych polskich banków.
- **Kanał rynkowy** globalny *risk-off* oznacza masową sprzedaż aktywów Europy Środkowej – deprecjacja złotego, odpływ z polskiego rynku obligacji; straty wycenowe w portfelach banków.
- **Kanał operacyjny:** banki same są intensywnymi konsumentami sprzętu IT opartego na chipach – trudności z wymianą i modernizacją infrastruktury, wydłużone cykle dostawy serwerów i bankomatów.
- **Kanał płynnościowy:** wzrost globalnych *spreadów* kredytowych i awersji do ryzyka podnosi koszt hurtowego finansowania polskich banków.
- **Kanał makroekonomiczny:** Recesja w Polsce – spadek PKB i wzrost bezrobocia; Chiny dokonują wyprzedaży polskich obligacji (retorsje en bloc wobec UE); trudniejsze plasowanie długu polskiego na rynkach.

4. Łączne potencjalne następstwa

- Najdłuższy horyzont oddziaływania spośród wszystkich scenariuszy: odbudowa zdolności produkcji zaawansowanych chipów poza Tajwanem zajęłaby lata; recesja przemysłowa w Polsce mogłaby trwać 3–5 lat.

- Trwała restrukturyzacja portfeli kredytowych: banki z dużą ekspozycją na przemysł motoryzacyjny i elektroniczny zmuszone do przeprojektowania strategii sektorowych.
- Impuls do reindustrializacji jako długoterminowa szansa: banki finansujące budowę lokalnych zdolności produkcji chipów (European Chips Act) zyskują nowy, długoterminowy strumień kredytów inwestycyjnych.
- Konieczność wbudowania ryzyka geopolitycznych łańcuchów dostaw w standardowe modele.
- Spadek CET1; prawdopodobny spadek rentowności banków nawet w średnim i długim horyzoncie.

SCENARIUSZ 12 Perfect Storm (kumulacja)

Kanał	Horyzont	Wpływ ogólny
wszystkie jednocześnie	natychmiast	krytyczny

1. Uzasadnienie wystąpienia scenariusza

- Dotychczasowe scenariusze traktują poszczególne ryzyka jako izolowane – tymczasem są one strukturalnie współzależne i wzajemnie się wzmacniają; zjawisko polikryzysów (permakryzysu)
- Wysoka współzależność globalnego systemu finansowego oznacza, że szok w jednym węźle natychmiast przenosi się na inne – próg tzw. kaskady systemowej jest niższy niż kiedykolwiek wcześniej.
- Polska jest w szczególnej pozycji: kraj flankowy NATO, poza strefą euro, silnie uzależniony od eksportu, z dużym udziałem kapitału zagranicznego w sektorze bankowym.
- Scenariusz *Perfect Storm* nie wymaga celowej koordynacji – wystarczy niekorzystna zbieżność czasowa autonomicznych procesów.

2. Scenariusz – przebieg wydarzeń

- **Zapalnik (*trigger*) finansowy:** globalny rynek nieruchomości komercyjnych lub obligacji korporacyjnych przeżywa gwałtowną korektę; kilka banków upada, wywołując efekt zarażania i wzrost spreadów na rynkach międzybankowych.
- **Zapalnik (*trigger*) geopolityczny:** w tym samym oknie czasowym dochodzi do eskalacji militarnej na wschodniej flance; USA sygnalizują ograniczone zaangażowanie; rynki wyceniają podwyższone ryzyko konfliktu.
- **Zapalnik (*trigger*) technologiczny:** skoordynowany cyberatak na infrastrukturę krytyczną kilku krajów UE powoduje wielodniowe zakłócenia w rozliczeniach transakcji i dostępie do bankowości elektronicznej.
- Trzy zapalniki nakładają się na siebie w ciągu 4–6 tygodni; razem tworzą spiralę wzajemnego wzmacniania: kryzys finansowy podważa zaufanie, napięcie geopolityczne blokuje koordynację polityczną, cyberatak uniemożliwia działanie infrastruktury.
- Polska doświadcza jednocześnie: odpływu kapitału, deprecjacji złotego, zakłóceń operacyjnych i presji budżetowej wynikającej z konieczności reagowania na trzy fronty.

3. Główne kanały transmisji i skutki dla banków

- **Kanał płynnościowy:** jednoczesne zamrożenie rynku międzybankowego, wzrost *spreadów bid-ask* i odpływ depozytów; NBP uruchamia awaryjne linie repo i swapy walutowe.
- **Kanał operacyjny:** systemy płatnicze (Elixir, Express Elixir, SORBNET2) zaatakowane lub w trybie awaryjnym; bankowość elektroniczna i mobilna niedostępna przez kilka dni.
- **Kanał kredytowy:** gwałtowny wzrost NPL, straty na portfelach obligacji skarbowych, pogorszenie się wskaźników kapitałowych; możliwe naruszenie buforów przez słabsze instytucje.
- **Kanał zaufania i reputacji:** jednoczesne zakłócenia operacyjne i informacje o problemach finansowych wywołują efekt runu na banki– nawet solidne banki tracą płynność wskutek paniki depozytariuszy; ogólny kryzys zaufania do instytucji politycznych i gospodarczych.

4. Łączne potencjalne następstwa

- Systemowy test odporności w warunkach rzeczywistych: wszystkie bufory, plany naprawy i procedury kryzysowe aktywowane i testowane jednocześnie.
- Trwała zmiana modelu operacyjnego: priorytetyzacja odporności nad efektywnością – wyższe wymogi płynnościowe, redundancja systemów IT, większe zapasy gotówki w obiegu.
- Sektor bankowy staje się elementem infrastruktury bezpieczeństwa państwa.
- Katalizator debaty o złotym i strefie euro: „strefa euro dałaby nam tarczę" vs. „własna waluta dała nam elastyczność" – wynik debaty będzie miał długofalowe konsekwencje dla architektury monetarnej Polski.

Ekspozycja na ryzyko geopolityczne w polskim systemie bankowym

Zbiorcza tabela ocen scenariuszy

Scenariusz	Główny kanał transmisji	Horyzont	Płynność	Kredyt (NPL)	Operac.	Kapitał	Wpływ ogólny
Eskalacja wojny na Ukrainie	makro + płynność + operacyjny	teraz	●●●	●●●	●●●	●●●	KRYTYCZNY
Wycofanie się USA z Europy	makro + rynkowy + cyber	1–3 lata	●●○	●●○	●●○	●●○	POWAŻNY
Kryzys i fragmentacja Unii Europejskiej	rynkowy + regulacyjny + makro	3–7 lat	●●○	●●●	●○○	●●○	POWAŻNY
Cyfrowe euro – fiasko implementacji	zaufania i reputacji + łańcuchów dostaw i powiązań	3–7 lat	●○○	●○○	●○○	●○○	UMIARKOWANY
Waluta BRICS – The Unit (dekompozycja systemu walutowego)	rynkowy + operacyjny	5–10 lat	●●○	●○○	●●○	●○○	UMIARKOWANY
Cyberatak na krajową infrastrukturę płatniczą	cyberbezpieczeństwa + zaufania i reputacji + płynnościowy	teraz	●●●	●○○	●●●	●●○	KRYTYCZNY
Cyberatak na infrastrukturę IT USA	operacyjny + rynkowy + łańcuchów dostaw i powiązań	teraz	●●○	●○○	●●●	●○○	POWAŻNY
Kryzys zaufania do AI w sektorze finansowym	operacyjny + regulacyjny + zaufania i reputacji	1–5 lat	●○○	●●○	●●●	●●○	POWAŻNY
Kryzys energetyczny 2.0 – permanentna drożyzna energii	kredytowy + makro	trwały	●○○	●●●	●○○	●●○	POWAŻNY
Dezintegracja łańcuchów dostaw – nowy protekcjonizm	kredytowy + powiązań i łańcuchów dostaw	trwały	●○○	●●●	●○○	●●○	POWAŻNY
Eskalacja konfliktu wokół Tajwanu z szokiem podażowym	rynkowy + kredytowy + makro	3–7 lat	●●○	●●●	●●○	●●○	KRYTYCZNY
Perfect Storm (kumulacja negatywnych zdarzeń/ wyzwalaczy ryzyka geopolitycznego)	wszystkie jednocześnie	teraz	●●●	●●●	●●●	●●●	KRYTYCZNY

Uwaga metodologiczna: oceny mają charakter ekspercko-jakościowy i nie wynikają z formalnego modelu kwantyfikacji, lecz z analizy kanałów transmisji ryzyka geopolitycznego i struktury ryzyka polskiego sektora bankowego. Każda ocena jest weryfikowalna przez odwołanie do kryteriów decyzyjnych poniżej.

Kryteria decyzyjne dla czterech skal ryzyka

Każda skala zakotwiczona jest w konkretnych mechanizmach regulacyjnych lub operacyjnych, co pozwala na weryfikację przyznanych ocen.

1. Ryzyko płynności

●●● **Wysokie**	Możliwość natychmiastowego zamrożenia rynku międzybankowego lub masowego odpływu depozytów; bank traci dostęp do finansowania hurtowego w ciągu 24–72 h; możliwe uruchomienie ELA przez NBP.
●●○ **Średnie**	Podwyższony koszt finansowania hurtowego i odpływ depozytów niestabilnych (instytucjonalnych); bufory płynnościowe (LCR) pod presją, ale bez bezpośredniego zagrożenia niewypłacalnością płynną.
●○○ **Niskie**	Marginalne napięcia płynnościowe możliwe w skrajnych podscenariuszach; standardowe bufory LCR/NSFR wystarczają do absorpcji szoku bez interwencji regulatora.

2. Ryzyko kredytowe (NPL)

●●● **Wysokie**	Skokowy wzrost NPL przekraczający zdolność absorpcji bieżących rezerw; konieczność tworzenia znaczących odpisów obniżających wynik netto i erodujących kapitał; restrukturyzacja portfeli o znacznej skali.
●●○ **Średnie**	Stopniowy wzrost NPL w jednym lub kilku sektorach portfela; rezerwy pod presją, ale wynik finansowy banku pozostaje dodatni; możliwe zawieszenie dywidend i wzrost kosztu ryzyka.
●○○ **Niskie**	Pogorszenie jakości portfela widoczne głównie w scenariuszach stress-testowych; w warunkach bazowych istniejące rezerwy i bufory kapitałowe w pełni absorbują wzrost NPL.

3. Ryzyko operacyjne

●●● **Wysokie**	Zakłócenia lub niedostępność kluczowych systemów (core banking, rozliczenia, kanały zdalne) przez ponad 24h; niemożność realizacji podstawowych funkcji bankowych; aktywacja planów ciągłości działania (BCP/DRP).
●●○ **Średnie**	Podwyższone koszty operacyjne i *compliance*; możliwe incydenty w systemach drugorzędnych lub przejściowe spowolnienie procesów; brak zakłóceń w obsłudze klienta, ale widoczna presja na zasoby IT i kadrę.
●○○ **Niskie**	Konieczność aktualizacji procedur i planów awaryjnych; brak bezpośrednich zakłóceń operacyjnych; ewentualne koszty dostosowawcze o charakterze jednorazowym i możliwym do za-planowania.

4. Ryzyko kapitałowe/wypłacalność

●●● **Wysokie**	Realne ryzyko naruszenia minimalnych wymogów kapitałowych (CET1, MREL); konieczność awaryjnego dokapitalizowania lub uruchomienia planów naprawy; możliwa interwencja KNF/BFG lub scenariusz resolution.
●●○ **Średnie**	Erozja buforów kapitałowych powyżej wymogów minimalnych (bufor ochrony kapitału, antycykliczny, O-SII); presja na wskaźniki adekwatności bez naruszenia progów regulacyjnych; ograniczenia dystrybucji zysku.
●○○ **Niskie**	Nieznaczne pogorszenie wskaźników kapitałowych mieszczące się w granicach buforów regulacyjnych; brak konieczności działań naprawczych; wpływ widoczny głównie w stress-testach EBA/KNF.

Wzajemne zależności. Scenariusze nie są niezależne: eskalacja konfliktu na Ukrainie podnosi prawdopodobieństwo cyberataku na infrastrukturę PL; kryzys energetyczny 2.0 wzmacnia presję na dezintegrację łańcuchów dostaw. *Perfect Storm* zakłada równoczesne zmaterializowanie się wyzwalaczy (*triggerów*) finansowych, geopolitycznych i technologicznych. W warunkach napięcia geopolitycznego korelacje między rodzajami ryzyka rosną, a dywersyfikacja traci skuteczność.

Rekomendacje dla dalszej analizy:

(1) Szacunki prawdopodobieństwa wystąpienia poszczególnych scenariuszy.

(2) Przekształcenie ocen jakościowych w parametry ilościowe dla scenariuszy o najwyższym priorytecie.

(3) Stress-testy bilansowe dla scenariuszy krytycznych zgodnie z metodologią EBA.

(4) Analiza wrażliwości na kluczowe założenia – w szczególności dotyczące skali odpływu depozytów i zdolności absorpcyjnej buforów kapitałowych.

(5) Weryfikacja i aktualizacja ocen w cyklu rocznym lub przy istotnych zmianach w otoczeniu geopolitycznym.

Spis tabel

Spis wykresów

Spis rysunków

Bibliografia

Ahn, J., Carton, B., Habib, A., Malacrino, D., Muir, D., & Presbitero, A. (2023). Geoeconomic fragmentation and foreign direct investment. W: World Economic Outlook, April 2023: A Rocky Recovery (s. 121–158). International Monetary Fund. https://doi.org/10.5089/9798400224119.081.

Aiyar, S., Malacrino, D., & Presbitero, A. F. (2024). *Investing in Friends: The Role of Geopolitical Alignment in FDI Flows*. International Monetary Fund.

Alison, G. (2018). *Skazani na wojnę? Czy Ameryka i Chiny unikną pułapki Tukidydesa?* Pascal.

Alsadan, A., Alalmaee, H., Zehri, C., & Ajili Ben Youssef, W. (2025). Global financial fragmentation under raised geopolitical risk. *International Economics and Economic Policy*, 22, 44. https://doi.org/10.1007/s10368-025-00671-x.

Alsadan, A., Alalmaee, H., Zehri, C., Youssef, W. (2025). Global financial fragmentation under raised geopolitical risk. *Int Econ Econ Policy*, 22 (44): 1–32.

Baker, S., Bloom, N., Davis S. (2016). Measuring Economic Policy Uncertainty, *The Quarterly Journal of Economics*, 131 (4): 1593–1636.

Bello, W. (2004). *Deglobalization. Ideas for a New World Economy*, London – New York.

BFG (2025). *Sytuacja finansowa w sektorze bankowym*. Wrzesień 2025. Warszawa.

BIS (2024). Deconstructing global trade: the role of geopolitical alignment, BIS Quarterly Review.

BiTBO. (2025). Bitcoin holdings of countries & governments. https://bitbo.io/treasuries/countries/.

Braudel F. (1992), *Kultura materialna, gospodarka i kapitalizm*, t. I–III, red. J. Kochanowicz, tłum. M. Ochab, P. Graff, Warszawa: Państwowy Instytut Wydawniczy.

Braudel F. (2006), *Gramatyka cywilizacji*, tłum. H. Igalson-Tygielska, Warszawa: Oficyna Naukowa.

Braudel, F. (1971). *Historia i trwanie*, tłum. B. Geremek, Czytelnik Warszawa, 1971.

Buch C. (2024). *Global rifts and financial shifts: supervising banks in an era of geopolitical instability.* Keynote speech by Claudia Buch, Chair of the Supervisory Board of the ECB, at the eighth European Systemic Risk Board (ESRB) annual conference on "New Frontiers in Macroprudential Policy".

Caldara, D. and Iacoviello, M. (2022). Measuring geopolitical risk. *American Economic Review*, Vol. 112, No 4, pp. 1194–1225.

Caldara, D., Conlisk, S., Iacoviello, M., Penn, M. (2022). The Effect of the War in Ukraine on Global Activity and Inflation URL: https://ideas.repec.org/p/fip/fedgfn/2022-05-27-2.html, doi:10.17016/2380-7172.3141.

Chainalysis. (2020). The KuCoin hack: What we know so far and how the hackers are using DeFi protocols to launder stolen funds. Chainalysis. https://www.chainalysis.com/blog/kucoin-hack-2020-defi-uniswap/.

Cheng, C.H.J., & Chiu, C.W. (2018). How important are global geopolitical risks to emerging countries? *International Economics*.

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). International Cybersecurity Law Review, 4(1), 79–90. https://doi.org/10.1365/s43439-022-00076-5.

Cole, E. (2013). The changing threat. In Advanced persistent threat (pp. 3–26). Elsevier. https://doi.org/10.1016/b978-1-59-749949-1.00001-2.

Collins English Dictionary 2023.

Conway, A. (2020). *New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security*. Microsoft Security Blog. Pobrano z https://www.microsoft.com/en-us/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/.

Cookson, J. A., Fox, C., Gil-Bazo, J., Imbet, J., & Schiller, C. (2023). *Social media as a bank run catalyst*. 22nd Annual FDIC Bank Research Conference. https://www.fdic.gov/analysis/cfr/bank-research-conference/annual-22nd/papers/cookson-paper.pdf.

Cope, Z. (2024). Introduction. In Z. Cope (Ed.), *The Palgrave handbook of contemporary geopolitics* (p. vii). Palgrave Macmillan.

Criekemans D. (2023). *Geopolitics, geoeconomics, and energy security in an age of transition towards renewables*, w: Handbook on the Geopolitics of the Energy Transition, Edited by Daniel Scholten, Edward Elgar Publishing, 2023.

Cybersecurity and Infrastructure Security Agency. (2022). Mis-, dis-, and malinformation (MDM) planning and incident response guide for election officials. https://web.archive.org/web/20220223192245/https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf.

CyBOK Project. (2021). Cyber Security Body of Knowledge (CyBOK) v1.1. https://www.cybok.org/knowledgebase1_1/.

Dieckelmann D. (i in.) (2024). Turbulent times: geopolitical risk and its impact on euro area financial stability ECB Financial Stability Review, maj.

Dodds, K. (2007). *Geopolitics. A very short Introduction*. Oxford University Press.

Drobiazko, A. O. (2024). The banking system of Ukraine as a factor of social stability in the war. Forum for Economic and Financial Studies, 2(2), 399. https://doi.org/10.59400/fefs.v2i2.399.

E&Y (2025). The 2025 Geostrategic Outlook.

ECB. (2024). Evolving IT and cybersecurity risks. ECB Banking Supervision. https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2024/html/ssm.nl241113_4.en.html.

ECB. (2026). T2 business continuity management. https://www.ecb.europa.eu/paym/target/t2/html/business-continuity-management.pl.html.

ENISA. (2022). European Cybersecurity Skills Framework (ECSF). https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.

ENISA. (2024). ENISA Threat Landscape: Finance Sector. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf.

ENISA. (2025). Technical implementation guidance: On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf.

ENISA. (2025a). Cybersecurity roles and skills for NIS2 essential and important entities. https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf.

ESRB. (2020). Systemic cyber risk. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

European Council. (2025). *Hybrid threats*. https://www.consilium.europa.eu/en/policies/hybrid-threats/.

Europejska Rada ds. Ryzyka Systemowego. (2021). Zalecenie Europejskiej Rady ds. Ryzyka Systemowego w sprawie ogólnoeuropejskich ram koordynacji dla właściwych organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17). Dziennik Urzędowy Unii Europejskiej, C 134, 1–10. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_134_R_0001.

Europejski Kongres Finansowy (2025). *Makroekonomiczne wyzwania i prognozy dla Polski*. XVI edycja – grudzień 2025.

Eurostat. (2026). *Government expenditure on defence*. Statistics Explained. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_on_defence.

Feng, C., Han, L., Vigne, S., & Xu, Y. (2023). Geopolitical risk and the dynamics of international capital flows. *Journal of International Financial Markets, Institutions & Money*, 82, 101693. https://doi.org/10.1016/j.intfin.2022.101693.

Forbes. (2025). Cryptocurrency prices today by market cap. https://www.forbes.com/digital-assets/crypto-prices/.

Fraser, N. (2015). Legitimation Crisis? On the Political Contradictions of Financialized Capitalism. *Critical Historical Studies*, 2:2, 157–189. https://www.journals.uchicago.edu/doi/abs/10.1086/683054.

Fundacja Bezpieczna Cyberprzestrzeń. (2024). Raport z ćwiczeń Cyber-EXE Polska 2024. https://www.ey.com/content/dam/ey-unified-site/ey-com/pl-pl/insights/consulting/documents/ey-raport-cyber-exe-polska-2024.pdf.

Hassan, T., Hollander, S., van Lent, L., Tahoun, A. (2019). Firm-Level Political Risk: Measurement and Effects, *The Quarterly Journal of Economics*, 134 (4): 2135–2202.

https://sites.duke.edu/icbdata/

https://www.gdeltproject.org/

Ikenberry, G. (2013). *Po zwycięstwie. Instytucje, ograniczenia strategiczne i przebudowa porządku po wielkich wojnach*. Wydawnictwo WEI, Warszawa.

Instytut Cyberbezpieczeństwa. (2024). *Wojna informacyjna*. https://instytutcyber.pl/artykuly/wojna-informacyjna/.

International Monetary Fund. (2025). Euro Area: Publication of Financial Sector Assessment Program documentation–Technical note on cyber risk and financial stability-Selected issues in regulation and supervision (IMF Country Report No. 25/213). International Monetary Fund. https://doi.org/10.5089/9798229019873.002.

Introduction: Context and Drivers of Permacrisis *Omprakash Mishra, Souradeep Sen*, w: Omprakash Mishra,·Souradeep Sen, Editors, Global Political Economy, Geopolitics and International Security, The World in Permacrisis, Palgrave MacMilla, 2024.

Kaczor, K. (2022). Gold-plating – problem nadtranspozycji dyrektyw unijnych do krajowego porządku prawnego. *Folia Iuridica Universitatis Wratislaviensis*, vol. 11 (1), 76–98.

Kaspersky. (2015, February 17). The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide. https://www.kaspersky.com/about/press-releases/the-great-bank-robbery-carbanak-cybergang-steals-1bn-from-100-financial-institutions-worldwide.

Khanna, P. (2002). *Konektografia*. Wydawnictwo Nowej Konferedacji.

Klaus, B., & Wendelborn, J. (2025). Cyber threats to financial stability in a complex geopolitical landscape. Financial Stability Review. European Central Bank. Pobrano z https://www.ecb.europa.eu/press/financial-stability-publications/fsr/focus/2025/html/ecb.fsrbox202505_01~5b8c62e6c6.en.html.

Komisja Europejska. (2023). Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego oraz zmieniającego rozporządzenie (UE) nr 1093/2010 (COM(2023) 367 final, 2023/0210 (COD)). https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52023PC0367.

Komisja Europejska. (2024). Rozporządzenie Wykonawcze Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiające zasady stosowania dyrektywy NIS2 w zakresie wymagań technicznych i metodycznych dotyczących środków zarządzania ryzykiem cyberbezpieczeństwa. Dziennik Urzędowy Unii Europejskiej. https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32024R2690.

Kopiński, D. (2025). *Atrakcyjność inwestycyjna Polski na tle Europy Środkowo-Wschodniej*. Point Paper, nr 3, Polski Instytut Ekonomiczny, Warszawa.

Kotkin, J. (2020). The Coming of neofeudalism. Encounter Books.

Li, K., Wang, Y., & Tang, Y. (2021). DETER: Denial of Ethereum Txpool sERvices. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21) (pp. 1645–1667). Association for Computing Machinery. https://doi.org/10.1145/3460120.3485369.

Lisakiewicz, R. (2017). Podejście geoekonomiczne w badaniu polityki zagranicznej Federacji Rosyjskiej. *Stosunki Międzynarodowe* 53 (1), 75-95.

Lu, B., & Liu, W. (2024). Does Comprehensive Geopolitical Risk Deter FDI Outflows: Evidence from China. *Defence and Peace Economics*, 35(3), 383–399.

UNCTAD. (2024). *World Investment Report 2024: Investment facilitation and digital government*. Geneva: United Nations.

Luttwak, E. N. (1990). From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest*, 20, 17–23. http://www.jstor.org/stable/42894676.

Market Insights: Top Geopolitical Risks of 2025, https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk.

Mahbubani, K. (2023). Czy Chiny już wygrały? Wydawnictwo Nowej Konfederacji.

Mahbubani, K. (2025). Czy Zachód przegrał? Glowbook.

Marszałek, P. (2014). *Systemy pieniężne wolnej bankowości: koncepcje, cechy, zastosowanie*. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. Poznań.

Marszałek, P., & Szarzec, K. (2022). Digitalization and the Transition to a Cashless Economy. W M. Ratajczak-Mrozek & P. Marszałek (Redaktorzy), *Digitalization and Firm Performance. Examining the Strategic Impact*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-83360-2_10.

Mehar, M., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2017). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology*, 21(1), 19–32. https://doi.org/10.2139/ssrn.3014782.

Morin, E. and Kern, A.B. (1999). *Homeland earth: A manifesto for the new millennium*. Hampton Press, s. 74. Tooze, A. 2022, October 28. Welcome to the world of the polycrisis. Financial Times. https://www.ft.com/content/498398e7-11b1-494b-9cd3-6d669dc3de33.

Morozow, E. (2014). *To Save Everything, Click Here*. Penguin.

Narodowy Bank Polski. (2020). Ocena funkcjonowania polskiego systemu płatniczego w I półroczu 2020 r. https://nbp.pl/wp-content/uploads/2022/09/ocena2020_1.pdf.

Narodowy Bank Polski. (2021). Narodowa strategia bezpieczeństwa obrotu gotówkowego. https://nbp.pl/wp-content/uploads/2022/09/NSBOG.pdf.

Narodowy Bank Polski. (2021a). Raport o obrocie gotówkowym w Polsce w 2020 r. https://nbp.pl/wp-content/uploads/2022/09/raport-o-obrocie-gotowkowym-w-Polsce-2020.pdf.

Narodowy Bank Polski. (2023). Raport o obrocie gotówkowym w Polsce w 2022 r. https://nbp.pl/wp-content/uploads/2023/10/Raport-o-obrocie-gotowkowym-2022_internet.pdf.

Narodowy Bank Polski. (2024). Rozwój systemu finansowego w Polsce w 2023 r. https://nbp.pl/wp-content/uploads/2024/11/RozwojSystemuFinansowegowPolsce_2023.pdf.

Narodowy Bank Polski. (2025). Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2024 r. https://nbp.pl/wp-content/uploads/2025/05/Ocena-II-polrocze-2024-r.pdf.

Narodowy Bank Polski. (2025a). Raport o obrocie gotówkowym w Polsce w 2024 r. https://nbp.pl/wp-content/uploads/2025/09/Raport-OG_2024_PL.pdf.

Narodowy Bank Polski. (2025B). Rozwój systemu finansowego w Polsce w 2024 r. https://nbp.pl/wp-content/uploads/2026/01/RozwojSystemuFinansowegowPolsce_2024.pdf.

NASK. (2025). Dezinformacja, misinformacja i malinformacja – czym się różnią? https://www.nask.pl/magazyn/dezinformacja-misinformacja-i-malinformacja-czym-sie-roznia.

National Bank of Ukraine. (2022). Financial Stability Report. https://bank.gov.ua/admin_uploads/article/FSR_2022-H1_eng.pdf.

NATO. (2025). *Defence expenditures and NATO's 5% commitment*. https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment.

NBP. (2024). *Raport o stabilności systemu bankowego*, Warszawa, grudzień 2024.

NBP. (2025) *Raport o stabilności systemu bankowego*, Warszawa, czerwiec 2025.

NBP. (2025a). *Raport o stabilności systemu bankowego*, Warszawa, grudzień 2025.

NIST. (2011). Managing information security risk: Organization, mission, and information system view (NIST Special Publication 800-39). National Institute of Standards and Technology and U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf.

NIST. (2024). NIST Cybersecurity Framework 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

North D.C. (1981). *North, Structure and Change in Economic History*, W.W. Norton & Co, New York–London 1981, s. 21.

PAB WIB (2026). Wpływ czynników regulacyjnych i fiskalnych na wyniki finansowe banków w I kwartale 2025 roku. Nr. 10/2026, Warszawa.

Parlament Europejski i Rada Unii Europejskiej. (2007). Dyrektywa 2007/64/WE z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego. Dziennik Urzędowy Unii Europejskiej, L 319, 1–36. https://eur-lex.europa.eu/eli/dir/2007/64/oj.

Parlament Europejski i Rada Unii Europejskiej. (2015). Dyrektywa (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego. Dziennik Urzędowy Unii Europejskiej, L 337, 35–127. https://eur-lex.europa.eu/eli/dir/2015/2366/oj.

Parlament Europejski i Rada Unii Europejskiej. (2022). Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego. Dziennik Urzędowy Unii Europejskiej, L 333, 1–79. https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

Parlament Europejski i Rada Unii Europejskiej. (2022a). Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Dziennik Urzędowy Unii Europejskiej, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

Parlament Europejski i Rada Unii Europejskiej. (2023). Rozporządzenie (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów. Dziennik Urzędowy Unii Europejskiej, L 150, 40–205. https://eur-lex.europa.eu/eli/reg/2023/1114/oj.

Pawlonka, T. (2025). „Udział instrumentów dłużnych w aktywach banków prawie zrównał się z udziałem kredytów dla sektora niefinansowego". miesięcznik BANK, 27.01.2025 12:02; https://bank.pl/udzial-instrumentow-dluznych-w-aktywach-bankow-prawie-zrownal-sie-z-udzialem-kredytow-dla-sektora-niefinansowego/.

Pescaroli, G. Michael Nones, Luca Galbusera, David Alexander, (2018). Understanding and mitigating cascading crises in the global interconnected system. *International Journal of Disaster Risk Reduction*, Volume 30, Part B, 2018, Pages 159–163, ISSN 2212-4209, https://doi.org/10.1016/j.ijdrr.2018.07.004.

Pinchetti M. (2024). *Geopolitics, International Economics, Macroeconomics, Monetary Policy*. Bank of England.

Pinto, A. (2024). *The battle against politically motivated cyber attacks on banks*. Cyber News Centre. Pobrano z https://www.cybernewscentre.com/the-battle-against-politically-motivated-cyber-attacks-on-banks/.

Radware. (n.d.). The Lazarus Group (APT38): North Korean threat actor. https://www.radware.com/cyberpedia/ddos-attacks/the-lazarus-group-apt38-north-korean-threat-actor/.

Raport „Top geopolitical risks 2025", https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/03/top-geopolitical-risks-2025-web.pdf.

Ratajczak, M., Woźniak-Jęchorek, B. (2020). Rewolucje przemysłowe i ich wpływ na rozwój ekonomii. Studia BAS, 3(63), 25–41, https://doi.org/10.31268/StudiaBAS.2020.20.

Ratajczak, M. (2017). Finansjalizacja gospodarki: wymiary dyskusji. *Bezpieczny Bank*, nr 3(68).

Reuters. (2023). Hackers hit websites of Danish central bank, other banks. https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/.

Sandri, D., Grigoli, F., Gorodnichenko, Y., & Coibion, O. (2023, September 4). Keep calm and bank on: Panic-driven bank runs and the role of public communication (BIS Working Papers No. 1119). Bank for International Settlements. https://www.bis.org/publ/work1119.htm.

Schwab, K. (2016). *The Fourth Industrial Revolution*. Penguin.

Securelist. (2015). *The Great Bank Robbery: the Carbanak APT*. Kaspersky Lab. https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/.

Sharma, R. (2018). Bitcoin Gold hack shows 51% attack is real. Investopedia. https://www.investopedia.com/news/bitcoin-gold-hack-shows-51-attack-real/.

SIPRI: Stockholm International Peace Research Institute. (2025). *Trends in world military expenditure, 2024* (SIPRI Fact Sheet, April 2025). https://www.sipri.org/sites/default/files/2025-04/2504_fs_milex_2024.pdf.

Szczepańska, O. (2022). Polityka pieniężna i makroostrożnościowa w Polsce w reakcji na kryzys wywołany pandemią Covid-19. W M. Lusztyn (red.), Polska bankowość w czasie pandemii Covid-19: Wybrane zagadnienia (s. 60–81). Fundacja Centrum Myśli Strategicznych. https://fundacjacms.pl/wp-content/uploads/2022/11/Polska-bankowo%C5%9B%C4%87-w-czasie-pandemii.-Wybrane-zagadnienia-e-book-final.pdf.

Taleb, N. (2020). *Czarny łabędź. Jak nieprzewidywalne zdarzenia rządzą naszym życiem*. Zysk i S-ka.

The Global Risks Report 2025, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.

Tuominen, A. (2025). Improving banks' resilience to hybrid threats (speech). ECB Banking Supervision. https://www.bankingsupervision.europa.eu/press/speeches/date/2025/html/ssm.sp251118_1~76cac1785d.en.html.

UNCTAD. (2025). *World Investment Report 2025: International investment in the digital economy*. Geneva: United Nations.

Verizon. (2021). 2021 Data Breach Investigations Report. Pobrano z https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf.

Verizon. (2022). 2022 Data Breach Investigations Report. Pobrano z https://www.verizon.com/business/resources/reports/2022-data-breach-investigations-report-dbir.pdf.

Verizon. (2023). 2023 Data Breach Investigations Report. Verizon. Pobrano z https://www.verizon.com/business/resources/reports/2024-data-breach-investigations-report-dbir.pdf.

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon. Pobrano z https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.

Verizon. (2025). 2025 Data Breach Investigations Report. Verizon. Pobrano z https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf.

Voell, J. (2020). Ethereum Classic hit by third 51% attack in a month. CoinDesk. https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month.

Wainwright, Z. (2025). The increasing impact of Bitcoin's ancient supply. Fidelity Digital Assets. https://www.fidelitydigitalassets.com/research-and-insights/increasing-impact-bitcoins-ancient-supply.

Warren-Kachelein, M. (2022). Update: Crypto hackers exploit Ronin Network for $615 million. BankInfoSecurity. https://www.bankinfosecurity.com/crypto-hackers-exploit-ronin-network-for-615-million-a-18810.

WEF (2025). Global Cybersecurity Outlook 2025. Pobrano z https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

Wojtyna, A. (2002). Demokratyczna kontrola nad polityką banku centralnego – kontrowersje teoretyczne i wnioski dla Polski, *Ekonomista*, nr 5.

Wrufakis, J. (2024) Technofeudalizm. Glowbook.

Wucker, M. (2016). *The grey rhino*. St. Martins Press.

Yahoo Finance. (2025). Bitcoin USD price (BTC-USD). https://finance.yahoo.com/quote/BTC-USD/.

Yahoo Finance. (2025a). Ethereum USD price (ETH-USD). https://finance.yahoo.com/quote/ETH-USD/.

Yaish, A., Qin, K., Zhou, L., Zohar, A., & Gervais, A. (2024). Speculative denial-of-service attacks in Ethereum. In Proceedings of the 33rd USENIX Security Symposium (SEC '24) (Article 198, pp. 3531–3548). USENIX Association.

ZBP. (2025). Banki 2024., Warszawa, kwiecień.

Zuboff, S. (2020). *Wiek kapitalizmu inwigilacji*. Zysk i S-ka.

PROGRAM
ANALITYCZNO
BADAWCZY