Komentarze OSW

OŚRODEK STUDIÓW WSCHODNICH NUMER 646 28.02.2025 www.osw.waw.pl

# Odporność Unii Europejskiej i NATO w dobie multikryzysu

Łukasz Maślanka, Piotr Szymański

**Dwie najważniejsze dla Europy instytucje bezpieczeństwa – NATO i UE – przechodzą obecnie przez drugą w ciągu ostatnich dziesięciu lat serię działań na rzecz poprawy odporności kryzysowej państw i społeczeństw. Pierwsza nastąpiła po rosyjskiej aneksji Krymu – wówczas obie organizacje rozpoczęły wzmacnianie swojej świadomości sytuacyjnej i cyberbezpieczeństwa oraz walkę z dezinformacją. Jednym z kamieni milowych było przyjęcie przez Sojusz w 2016 r. siedmiu bazowych wymogów gotowości cywilnej. Aktualną wywołały pandemia COVID-19 i inwazja Rosji na Ukrainę. Wnioski z tej kumulacji kryzysów dotyczą m.in. rezerw strategicznych, wydolności opieki zdrowotnej, bezpieczeństwa dostaw, ochrony i ewakuacji ludności cywilnej oraz zwalczania operacji sabotażowo-dywersyjnych.**

**Pomysły Komisji Europejskiej (KE) zmierzają do całościowej poprawy odporności kryzysowej UE, ale w zakresie niewkraczającym w obronę zbiorową NATO. Wyrazem tych aspiracji jest zredagowany pod kierunkiem byłego prezydenta Finlandii Sauliego Niinistö i zaprezentowany przez KE w październiku 2024 r. raport poświęcony poprawie cywilno-wojskowej gotowości Europy. Z kolei Sojusz dwa miesiące później zapowiedział aktualizację swojej strategii zwalczania zagrożeń hybrydowych. Obie organizacje powinny nadal jak najściślej koordynować swoje poczynania w tej dziedzinie, dążąc do uzyskania synergii oraz unikając niepotrzebnego duplikowania struktur i konkurowania.**

## Bezpieczeństwo całościowe według Unii

Od ponad dekady UE rozwija instrumenty wzmacniające odporność państw członkowskich w różnych obszarach. W latach 2008–2022 obowiązywał program ochrony infrastruktury krytycznej, koncentrujący się na sektorach energetycznym i transportowym. Wraz z przyjęciem Dyrektywy CER (o odporności podmiotów krytycznych)[1] w 2022 r. rozszerzono go o bankowość, infrastrukturę rynków finansowych, zdrowie, wodę pitną, ścieki, infrastrukturę cyfrową, administrację publiczną, przestrzeń kosmiczną oraz wytwarzanie, przetwarzanie i dystrybucję żywności. Dokument ten wprowadza zharmonizowane normy minimalne, które mają pozwolić na zapewnienie ciągłości świadczenia kluczowych usług oraz zwiększenie odporności podmiotów krytycznych (świadczących usługi w wymienionych sferach). Za niewywiązywanie się z obowiązków grożą im ze strony krajów unijnych sankcje finansowe.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG), eur-lex.europa.eu.

OSW

Ośrodek Studiów Wschodnich im. Marka Karpia
ul. Koszykowa 6a, 00-564 Warszawa
tel.: (+48) 22 525 80 00, info@osw.waw.pl
www.osw.waw.pl

REDAKCJA MERYTORYCZNA: Justyna Gotkowska
REDAKCJA: Tomasz Strzelczyk, Szymon Sztyk
SKŁAD: Wojciech Mańkowski

Równocześnie podmioty krytyczne mogą ze względów bezpieczeństwa uzyskać od państwa wsparcie, które nie będzie traktowane jako niedozwolona pomoc publiczna. Ponadto od 2001 r. funkcjonuje i jest rozwijany Unijny Mechanizm Ochrony Ludności, koordynujący pomoc ratowniczą i humanitarną w razie wystąpienia katastrofy naturalnej.

Od 2014 r. UE dąży do osiągnięcia zdolności odpowiadania na zagrożenia hybrydowe w sferach zwalczania broni masowego rażenia, bezpieczeństwa dostaw energii, bezpieczeństwa morskiego, ochrony danych, ochrony granic unijnych, kosmicznej czy zagranicznych inwestycji bezpośrednich. W budowaniu jej odporności na znaczeniu zyskały poprawianie świadomości sytuacyjnej, cyberbezpieczeństwo oraz walka z dezinformacją. W 2019 r. Rada UE uznała, że „kraje członkowskie mają możliwość aktywowania unijnej klauzuli solidarności (art. 222 Traktatu o funkcjonowaniu UE) w odpowiedzi na poważny kryzys wynikający z aktywności hybrydowej". Nowy poziom ambicji w tym zakresie wyznaczył *Kompas strategiczny* z 2022 r. Zgodnie z nim kraje UE rozwijają narzędzia reagowania na działania hybrydowe (EU Hybrid Toolbox), w tym powołane do życia w 2024 r. zespoły szybkiego reagowania na zagrożenia hybrydowe (EU Hybrid Rapid Response Teams), przypominające funkcjonujące w NATO zespoły kontrhybrydowe.

**„ Komisja chce skuteczniej korzystać z istniejących narzędzi i instrumentów oraz uniknąć kontrowersyjnej dla niektórych państw zmiany traktatów.**

30 października 2024 r. KE opublikowała opracowany pod kierunkiem byłego prezydenta Finlandii Niinistö raport *Razem bezpieczniejsi. Wzmocnienie cywilnej i wojskowej gotowości kryzysowej Europy*[2]. Sporządzono go na wspólne zamówienie przewodniczącej Komisji Ursuli von der Leyen oraz wysokiego przedstawiciela UE ds. polityki zagranicznej i bezpieczeństwa Josepa Borrella. KE i Europejska Służba Działań Zewnętrznych (ESDZ) dążą tym samym do „skatalogowania" kompetencji Unii w szeroko rozumianej polityce bezpieczeństwa i relacjach zewnętrznych – dokument zawiera rekomendacje w ośmiu newralgicznych obszarach (zob. Aneks).

Komisja chce przede wszystkim skuteczniej korzystać z istniejących narzędzi i instrumentów oraz uniknąć kontrowersyjnej dla niektórych państw zmiany traktatów. Zwiększyć zdolności reagowania kryzysowego UE miałyby rozbudowa Centrum Koordynacji Reagowania Kryzysowego (ERCC), działającego w ramach Komisji od 2013 r., oraz usprawnienie mechanizmu reagowania kryzysowego (IPCR) przy Radzie UE. ERCC zyskałoby rolę centralnego hubu operacyjnego, swoistego „jednego okienka" reakcji na wszelkie kryzysy. Stopniowo przejmowałoby też inicjatywę od Rady UE, co eufemistycznie określono mianem „wzmacniania powiązań ze strukturami zarządzania kryzysowego wewnątrz ESDZ".

Raport Niinistö postuluje „dalszą operacjonalizację" art. 42.7 TUE (klauzuli wzajemnej obrony) oraz art. 222 TFUE (klauzuli solidarności). Ten pierwszy nakłada „obowiązek udzielenia pomocy i wsparcia przy zastosowaniu wszelkich dostępnych im środków" państwu członkowskiemu, które padło ofiarą agresji zbrojnej. Wśród krajów Unii nie ma jednak zgody na interpretację go w sposób zbliżony do art. 5 traktatu waszyngtońskiego. Rekomendacje odnośnie do tego przepisu są więc ogólne i kierują się w stronę wypracowania scenariuszy jego aktywowania oraz zdefiniowania roli UE w udzielaniu pomocy w razie agresji. W odniesieniu do art. 222 TFUE dokument sugeruje obniżenie „progu" jego uruchomienia (teraz istnieje wymóg niewystarczających sił i środków radzenia sobie z kryzysem po stronie państwa członkowskiego) i objęcie nim działań hybrydowych, sabotażowych, hakerskich czy pandemii.

[2] S. Niinistö, *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, Komisja Europejska, 30.10.2024, commission.europa.eu.

Raport zaleca powołać Instrument Obrony Europy (Defending Europe Facility) i Instrument Bezpieczeństwa Europy (Securing Europe Facility) jako oddzielną część budżetu grupującego wszystkie inwestycje UE w zakresie – odpowiednio – wsparcia przemysłu zbrojeniowego oraz ochrony ludności i reagowania kryzysowego. Wniosek ten odpowiada na propozycję KE dotyczącą centralizacji wszystkich celowych funduszy w tych dwóch obszarach. Przed zbliżającymi się negocjacjami wieloletnich ram finansowych (WRF) na lata 2028–2034 dokument postuluje uwzględnienie czynnika „gotowości kryzysowej" w konstruowaniu budżetu UE oraz większą elastyczność WRF i corocznych budżetów. Ma to pozwolić Komisji na swobodniejsze zarządzanie środkami i podwyższyć jej rangę jako dysponenta wsparcia.

## Ile NATO w zwalczaniu zagrożeń hybrydowych?

Pierwszą strategię zwalczania zagrożeń hybrydowych NATO przyjęło w 2015 r. w reakcji na anektowanie Krymu. Choć dokument jest poufny, to Sojusz zakomunikował, że jej filary to wzmacnianie gotowości do przeciwdziałania zagrożeniom hybrydowym (głównie ze strony Rosji i Chin), ich odstraszanie oraz obrona przed nimi[3]. Do priorytetów organizacji zaliczono: gromadzenie, analizę i wymianę informacji, wsparcie państw członkowskich w identyfikacji luk i zwiększaniu odporności, dostarczanie ekspertyzy w zakresie gotowości cywilnej, zwalczanie broni masowego rażenia, reagowanie kryzysowe, ochronę infrastruktury krytycznej, komunikację strategiczną, ochronę ludności, bezpieczeństwo energetyczne i zwalczanie terroryzmu. Od szczytu w Warszawie w 2016 r. Sojusz uznaje też, że atak hybrydowy może – podobnie jak cybernetyczny – aktywować art. 5. W 2017 r. w Kwaterze Głównej NATO powstał wydział ds. analiz zagadnień hybrydowych w nowym Połączonym Pionie Wywiadu i Bezpieczeństwa (Joint Intelligence and Security Division, JISD). Od 2018 r. Sojusz dysponuje eksperckimi zespołami wspomagającymi ds. zwalczania zagrożeń hybrydowych. Doradzają one władzom państwa, które zwróci się o ich pomoc. W 2019 r. mechanizm ten uruchomiła Czarnogóra, aby zabezpieczyć wybory parlamentarne, a w 2021 r. Litwa – po wybuchu kryzysu związanego z napływem migrantów przez granicę z Białorusią. W obliczu narastania wrogich działań nieregularnych w grudniu 2024 r. kraje NATO po spotkaniu ministrów spraw zagranicznych poinformowały o rozpoczęciu prac nad aktualizacją dotychczasowej sojuszniczej strategii zwalczania zagrożeń hybrydowych. Szczegółów proponowanych zmian nie ujawniono.

> **„Pierwszą strategię zwalczania zagrożeń hybrydowych NATO przyjęło w 2015 roku w reakcji na anektowanie Krymu przez Rosję.**

W ostatnim czasie na pierwszej linii frontu natowskiej walki z zagrożeniami hybrydowymi znalazła się ochrona podmorskiej infrastruktury krytycznej. To m.in. pokłosie uszkodzenia gazociągów Nord Stream 1 i 2 (2022) oraz Balticconnector (2023), kabla energetycznego Estlink2 (2024) oraz licznych kabli telekomunikacyjnych w 2024 r. W odpowiedzi jeszcze w 2024 r. powołano Centrum Bezpieczeństwa Krytycznej Infrastruktury Podmorskiej NATO w ramach Sojuszniczego Dowództwa Sił Morskich (MARCOM) oraz ekspercką Sieć Krytycznej Infrastruktury Podmorskiej NATO. W styczniu 2025 r. Naczelny Dowódca Sił Sojuszniczych w Europie (SACEUR) zadecydował o zwiększeniu aktywności patrolowej sojuszniczych jednostek powietrznych, nawodnych i podwodnych na Bałtyku, ukierunkowanej na ochronę podmorskiej infrastruktury krytycznej i odstraszanie kolejnych incydentów[4]. Kroki te pokazują zdolność NATO do szybkiego reagowania.

---

[3] E.H. Christie, K. Berzina, *NATO and Societal Resilience: All Hands on Deck in an Age of War*, German Marshall Fund, 20.07.2022, gmfus.org; A. Dowd, C. Cook, *Bolstering Collective Resilience in Europe*, Center for Strategic & International Studies, 9.12.2022, csis.org; *Countering hybrid threats*, NATO, 7.05.2024, nato.int.

[4] P. Szymański, *Wartownik Bałtyku: wzmocniona aktywność NATO na akwenie*, OSW, 15.01.2025, osw.waw.pl.

Podejście organizacji do zagrożeń hybrydowych pokrywa się częściowo z posunięciami na rzecz wzmocnienia całościowej odporności państw i społeczeństw na agresję. Mowa o przyjętych w 2016 r. w Warszawie siedmiu bazowych wymogach gotowości cywilnej NATO. Chodzi o: ciągłość rządów i podstawowych usług rządowych, odporne dostawy energii, zdolność do skutecznego radzenia sobie z niekontrolowanym przepływem osób, odporne zasoby żywności i wody, zdolność do radzenia sobie z ofiarami na masową skalę, odporne cywilne systemy łączności, odporne systemy transportu cywilnego. W 2017 r. NATO przyjęło kryteria oceny ich wdrażania, a rok później – wytyczne w tym zakresie dla sojuszników. W 2021 r. ustalono zobowiązanie do dalszego całościowego wzmacniania odporności na zagrożenia konwencjonalne, nieregularne i hybrydowe, terrorystyczne, cybernetyczne i informacyjne. W 2023 r. NATO zatwierdziło cele odporności kierunkujące rozwój zdolności cywilnych, a deklaracja z ostatniego szczytu w Waszyngtonie w 2024 r. mówi już wprost o włączeniu tych ostatnich do sojuszniczego planowania obronnego. Realnie działania organizacji na tym polu przez długi czas miały dosyć ograniczony zakres. Istotną rolę odgrywają jednak szkolenia i ćwiczenia oraz włączanie scenariuszy hybrydowych i współpracy z sektorem prywatnym do poligonowych ćwiczeń NATO.

> **W październiku 2024 roku sojusznicy wypracowali wspólne podejście do zwalczania zagrożeń informacyjnych.**

Równolegle stale rośnie znaczenie cyberobrony w NATO. Sojusz motywuje państwa członkowskie do większych inwestycji w cyberbezpieczeństwo, stanowi platformę wymiany informacji i szkoleniową, a także zabezpiecza własne sieci i wspiera bezpieczeństwo sieci krajowych. W 2023 r. przyjął nową koncepcję wprzęgnięcia tej domeny w sojusznicze odstraszanie i obronę. Aktualnie rozpoczyna proces łączenia rozproszonych zdolności w cyberprzestrzeni. Zapowiedziano sformowanie Zintegrowanego Centrum Obrony Cybernetycznej NATO – gotowość operacyjną ma ono osiągnąć w 2028 r.[5]

W październiku 2024 r. sojusznicy wypracowali także wspólne podejście do zwalczania zagrożeń informacyjnych. Ma ono umożliwić wczesne ostrzeganie przed wrogimi operacjami tego typu, skuteczniejszą odpowiedź na nie (m.in. poprzez proaktywną komunikację strategiczną), ich powstrzymywanie i mitygowanie (dzięki wspólnym oświadczeniom, sprostowaniom, zwalczaniu wrogiej narracji czy publicznej atrybucji). Przewodnią rolę koordynującą na tym polu ma odgrywać Komitet ds. Dyplomacji Publicznej NATO.

## Zwiększanie odporności UE: szanse, wyzwania i perspektywy

Raport Niinistö rozwija zapisy poprzednich dokumentów o podobnej tematyce – *Kompasu strategicznego*, deklaracji z Wersalu, *Europejskiej strategii przemysłowej w zakresie obronności* (EDIS) czy wytycznych politycznych przewodniczącej KE na lata 2024–2029. Można więc go uznać za część „mapy drogowej" dotyczącej budowy „europejskiej unii obronnej", rozumianej jako synergia działań KE na rzecz bezpieczeństwa z koordynowaną przez Radę UE wspólną polityką bezpieczeństwa i obrony (WPBiO). Zarazem ma on ukierunkować prace nad kolejnymi tekstami: *Strategią na rzecz Unii Gotowości* oraz *Białą księgą przyszłości europejskiej obronności*[6]. Jest też elementem strategii politycznej instytucji

[5] Sieci Sojuszu pilnuje Centrum Bezpieczeństwa Cybernetycznego NATO, które może też wydzielić zespoły szybkiego reagowania do pomocy zaatakowanemu państwu. W 2018 r. w SHAPE utworzono Centrum Operacji w Cyberprzestrzeni, odpowiedzialne za budowanie wspólnej świadomości sytuacyjnej, koordynację aktywności sojuszników oraz zabezpieczenie operacji natowskich. Zdolności odpowiedzi w tej domenie uległy dalszemu wzmocnieniu w 2022 r., gdy sojusznicy podjęli decyzję o powołaniu nowej zdolności szybkiego reagowania na złośliwe działania (*Virtual Cyber Incident Support Capability*). Jest to dobrowolna pomoc cybernetyczna udzielana sobie nawzajem przez państwa członkowskie w razie zgłoszenia takiej potrzeby.

[6] *White paper on the future of European defence*, Parlament Europejski, 5.11.2024, europarl.europa.eu.

unijnych nastawionej na uzyskanie od państw członkowskich nowych kompetencji i dodatkowego finansowania w celu sprawniejszego – w ich przekonaniu – prowadzenia przez organizację polityki w sferze bezpieczeństwa i relacji z partnerami oraz rywalami zewnętrznymi.

Raport może również dać impuls do dodatkowej aktywności legislacyjnej i regulacyjnej wyznaczającej wspólne dla wszystkich krajów UE minimalne normy zgodności z zasadami gotowości w takich sferach jak edukacja, magazynowanie rezerw, budownictwo (konstrukcja schronów), bezpieczeństwo energetyczne czy zamówienia publiczne. Przełom stanowiłoby wdrażanie rekomendacji dotyczących wprowadzenia unijnych regulacji w zakresie standardów i wymogów w obszarze gotowości kryzysowej, które nakładałyby na członków konkretne zobowiązania. Podobnie rozszerzenie ram ochrony infrastruktury krytycznej o przemysł zbrojeniowy generowałoby nowe obowiązki i koszty dla biznesu.

> **Implementacja dokumentu stwarza szansę na dodatkowe wsparcie ze strony UE również w obszarze ochrony granic zewnętrznych.**

Działalność legislacyjna UE zmierzająca do podwyższenia poziomu gotowości na zagrożenia w państwach organizacji dałaby asumpt do debaty wewnętrznej i współgrałaby z polskimi planami inwestycji w system ochrony ludności i obrony cywilnej. Zarazem raport Niinistö podkreśla znaczenie tak ważnego dla bezpieczeństwa wschodniej flanki zagadnienia jak mobilność wojskowa oraz zawiera perspektywy przeznaczania dodatkowych środków na kosztowne przedsięwzięcia (np. związane z uzupełnianiem rezerw strategicznych). Polskiej prezydencji w Radzie UE dostarcza więc następnego argumentu za promowaniem postulatów istotnych z punktu widzenia interesów państwa.

Implementacja (przynajmniej częściowa) dokumentu stwarza szansę na dodatkowe wsparcie UE również w obszarze ochrony granic zewnętrznych. O zmianie nastawienia KE w tej sprawie świadczy oświadczenie z 11 grudnia[7], w którym przyznaje krajom członkowskim prawo do powoływania się na postanowienia Traktatu, aby ograniczać prawo do azylu, jeżeli migrację wywołano celowo, a także zapowiada dalszą pomoc w zabezpieczeniu granic zewnętrznych.

Urzeczywistnianie rekomendacji raportu może napotkać liczne przejawy oporu. Niektóre stolice mogą mieć wątpliwości, czy zasadne jest nadmierne rozwijanie struktur reagowania kryzysowego w ESDZ czy KE. Może to też komplikować bieżącą kooperację pomiędzy UE i NATO. Nawet jeżeli hasło „pełnoprawnej unijnej służby ds. współpracy wywiadowczej" wyznacza horyzont dalekich ambicji Brukseli, to część państw może sprzeciwiać się rozwijaniu tego typu współdziałania w UE (chodzi zwłaszcza o dzielenie się wrażliwymi informacjami w narażonym na penetrację przez wrogie służby środowisku instytucji unijnych i niektórych członków).

W zakresie diagnozy zagrożeń KE ogranicza się do zgody na ich wyczerpujące wyliczenie, podczas gdy prawdziwy problem stanowi wspólne ustalenie stopnia ich bliskości i priorytetów. Część krajów może choćby uznać, że atrybucja ataków hybrydowych lub – tym bardziej – podejmowanie działań odwetowych nie powinno następować na poziomie UE. Wreszcie – wszelkie sugestie raportu niosące za sobą dodatkowe koszty mogą budzić niechęć państw „oszczędnych". Propozycja uzależnienia dystrybucji niektórych funduszy unijnych od realizacji zadań z zakresu gotowości kryzysowej wygląda zaś jak powoływanie kolejnego narzędzia rozszerzającego pole arbitralności decyzyjnej KE.

Ryzyka związane z wdrożeniem dokumentu wpisują się w szerszy katalog obaw dotyczących przekazywania instytucjom unijnym dalszych kompetencji i inspirowania ich do posunięć prowadzących

[7] *Communication on countering hybrid threats from the weaponisation of migration and strengthening security at the EU's external borders*, Komisja Europejska, 11.12.2024, eur-lex.europa.eu.

do centralizacji polityki bezpieczeństwa kosztem państw członkowskich oraz kompetencji innych organizacji (zwłaszcza NATO). Istnieje też niebezpieczeństwo odgórnego ustalania norm i wymuszania ich implementacji w sposób niebiorący pod uwagę specyficznych uwarunkowań bezpieczeństwa konkretnych krajów. Problemem może się także okazać nadmiernie ambitne zakreślenie przez KE obszaru przyszłych regulacji bez pewności uzyskania finansowania na ich realizację.

> **Przyjęcie nowej *Koncepcji strategicznej NATO* w 2022 roku nie przyniosło przełomu w sojuszniczym podejściu do odporności.**

Istotne, że raport podkreśla konieczność ściślejszej współpracy UE z NATO i nie wikła się w dzielące sojuszników rozważania o europejskiej autonomii strategicznej. Zachowuje również wstrzemięźliwość w programowaniu kooperacji UE–USA. Definiuje Rosję jako pierwszoplanowe zagrożenie, co wskazuje na zbieżność ocen w tej sferze z natowskimi. Niektóre postulaty w nim zawarte świadczą o pewnym naśladowaniu rozwiązań funkcjonujących w Sojuszu – jak choćby propozycja przyjęcia wytycznych dotyczących gotowości (*Preparedness Baseline Requirements*), przypominających siedem bazowych wymogów gotowości cywilnej w NATO[8]. Synergia działań z zakresu niemilitarnej odporności kryzysowej państw i społeczeństw stanowi perspektywiczne pole współdziałania UE i NATO (np. w odniesieniu do rezerw strategicznych). Komunikację między oboma organizacjami w kluczowych kwestiach bezpieczeństwa może ułatwić zwiększenie roli Komisji.

Znaczenie dla obrony zbiorowej i regionalnych planów obronnych Sojuszu mają fragmenty raportu dotyczące szeroko rozumianego wsparcia logistycznego ze strony UE. Obejmuje ono wzmocnienie mobilności wojskowej, ochrony infrastruktury krytycznej, partnerstwa z sektorem prywatnym i rezerw strategicznych. Budowaniu sił do wypełnienia owych planów sprzyjałaby realizacja rekomendacji dokumentu w sferach inwestycji w przemysł obronny oraz wspomagania zatrudnienia w dziedzinie bezpieczeństwa.

## Zwiększanie odporności NATO i korelacja z UE

Przyjęcie nowej *Koncepcji strategicznej NATO* w 2022 r. nie przyniosło przełomu w sojuszniczym podejściu do odporności. Nie zdefiniowano jej wówczas jako czwartego głównego zadania Sojuszu – obok odstraszania i obrony, zapobiegania kryzysom i zarządzania nimi oraz budowania bezpieczeństwa opartego na współpracy. Liczne dyskusje nie doprowadziły też do rozszerzenia katalogu siedmiu bazowych wymogów odporności (np. o systemy płatnicze, obronę psychologiczną i oprogramowanie) czy ewolucji natowskiego Euroatlantyckiego Ośrodka Koordynacji Reagowania w przypadku Katastrof w kierunku sojuszniczej agencji rezerw materiałowych (na fali działań przeciwpandemicznych). Zasadniczo posunięcia Komitetu ds. Odporności NATO mają motywować państwa członkowskie do planowania, wdrażania i raportowania zdolności cywilnych, ale stolice otrzymały w tym zakresie znaczną swobodę. Brak tu zaawansowanego narzędzia porównywalnego do procesu planowania obronnego (NDPP) i mechanizmu kontrolnego. Kooperację w obszarze bazowych wymogów odporności utrudniają: niechęć rządów do dzielenia się informacjami na temat wrażliwych elementów narodowych systemów bezpieczeństwa, znaczne dysproporcje między poszczególnymi państwami w zarządzaniu rezerwami strategicznymi czy obronie cywilnej oraz komplikacje budżetowe – wydatki na szeroko rozumianą odporność są „zaparkowane" w wielu resortach. Odbudowa zdolności w zakresie niemilitarnej odporności na agresję w Europie będzie procesem żmudnym ze względu na pozimnowojenne oszczędności w tej dziedzinie oraz prywatyzację, która pozbawiła członków licznych dostępnych wcześniej narzędzi.

[8] W.-D. Roepke, H. Thankey, *Odporność – pierwsza linia obrony*, „Przegląd NATO", 27.02.2019, nato.int.

W NATO odpowiedzialność za reakcję na atak hybrydowy spoczywa przede wszystkim na barkach poszczególnych krajów, a jej skuteczność w największym stopniu zależy od ich indywidualnych zdolności. Sojusz pełni funkcję pomocniczą, a oprócz tego uruchomienie części środków umożliwiających odpowiedź na zagrożenia tego typu potrzebuje zgody Rady Północnoatlantyckiej, co może spowalniać udzielenie pomocy. Takiej autoryzacji wymagało choćby wysłanie w 2021 r. natowskiego zespołu kontrhybrydowego na Litwę. Równocześnie w ostatnich latach poszerzono swobodę SACEUR-a w podejmowaniu wzmożonej aktywności sił sojuszniczych (np. Baltic Sentry) i w dysponowaniu natowskimi siłami odpowiedzi (Allied Reaction Force), co wzmacnia odstraszanie przed agresją hybrydową na większą skalę.

**” Zapowiadana przez sojuszników aktualizacja strategii hybrydowej NATO powinna uwzględniać nowe zagrożenia.**

Zagrożenia hybrydowe i terrorystyczne oraz odporność stały się głównymi obszarami zacieśniania współpracy UE z NATO już w latach 2016–2017. Trwa regularna wymiana informacji między różnymi ciałami unijnymi i natowskimi oraz kooperacja w ramach Europejskiego Centrum Doskonałości ds. Przeciwdziałania Zagrożeniom Hybrydowym w Helsinkach. Od 2022 r. strony prowadzą ustrukturyzowany dialog na temat odporności, a od 2024 r. – również cyberbezpieczeństwa. Celem jest konsolidowanie ich poczynań. W styczniu 2023 r. utworzono wspólną Grupę Zadaniową ds. Odporności Infrastruktury Krytycznej, która przedstawiła rekomendacje dotyczące ochrony infrastruktury energetycznej, transportowej, cyfrowej i kosmicznej. Struktury obu organizacji kooperują ze sobą w tym zakresie dość harmonijnie. W przeciwieństwie do NATO UE wolno nakładać sankcje na państwa i podmioty dopuszczające się szkodliwych działań hybrydowych. NATO jako sojusz wojskowy może zaś zadecydować o uruchomieniu operacji militarnej o charakterze prewencyjnym (np. w obliczu niebezpieczeństwa dla infrastruktury morskiej czy na granicy między państwem sojuszniczym a krajem stanowiącym zagrożenie), a także wysłać zespoły doradcze.

Aktualizacja strategii hybrydowej NATO powinna uwzględniać nowe zagrożenia. Szczególny nacisk należy położyć na ochronę podmorskiej infrastruktury krytycznej, w tym na wypracowanie metod postępowania w przypadku wydarzenia poza wodami terytorialnymi, a więc poza obszarem jurysdykcji państwa. Kolejna istotna sprawa to przeciwdziałanie rosyjskiemu zagłuszaniu sygnału GPS (np. poprzez inwestycje w inercyjne systemy nawigacji). Nowa strategia mogłaby też motywować państwa członkowskie do inwestycji w agencje bezpieczeństwa wewnętrznego oraz obejmować wykorzystanie narzędzi oferowanych przez sztuczną inteligencję do wczesnej identyfikacji zagrożeń w połączeniu z podniesieniem nakładów na monitoring obszaru traktatowego (systemy satelitarne i bezzałogowe). Równocześnie – wbrew deklarowanym aspiracjom NATO – trudno będzie odgrywać większą rolę na froncie walki z dezinformacją. Sojusz powinien pozostać skoncentrowany na własnej komunikacji strategicznej. Aktualizowaną strategię może uzupełniać koncepcja odporności warstwowej, opracowywana przez Sojusznicze Dowództwo ds. Transformacji (ATC), która zakłada wzajemne przenikanie się i wzmacnianie gotowości cywilnej i militarnej[9].

[9] *NATO Warfighting Capstone Concept*, Sojusznicze Dowództwo ds. Transformacji, 2021, act.nato.int; *The Layered Resilience Concept*, „CIMIC Handbook”, 20.08.2024, handbook.cimic-coe.org.

# ANEKS

**Wybrane propozycje działań zawarte w raporcie Niinistö**

| Obszar | Działania |
|---|---|
| **1. Odporność kryzysowa UE** | • **stworzenie unijnej oceny ryzyk (*EU Risk Assessment*)**<br>• **wzmocnienie gotowości kryzysowej Unii – przygotowanie *Strategii na rzecz Unii Gotowości*:**<br>- zdefiniowanie krytycznych obszarów funkcjonowania społeczeństw i administracji na szczeblu unijnym,<br>- stworzenie wymogów w zakresie gotowości do każdego z tych krytycznych obszarów (*Preparedness Baseline Requirements*),<br>- zakorzenianie w UE myślenia i działania w kategoriach gotowości,<br>- obowiązkowa analiza aktów prawnych UE pod kątem wpływu na gotowość kryzysową,<br>- jasny podział kompetencji w dziedzinie reagowania kryzysowego i gotowości w ramach UE,<br>- wprowadzenie unijnych ćwiczeń testowania procesu decyzyjnego w sferze gotowości kryzysowej<br>• **analiza możliwości wprowadzenia unijnego prawa względem standardów i wymogów dla państw członkowskich w obszarze gotowości kryzysowej**<br>• **wypracowanie jasnej wizji roli UE w pomocy członkowi, który padł ofiarą agresji zbrojnej**<br>• **wzmocnienie współpracy z NATO, m.in. poprzez uzgodnienie protokołu kryzysowego uruchamiającego zwiększony przepływ informacji na linii UE–NATO** |
| **2. Szybkość działań** | • **zacieśnianie koordynacji:**<br>- powołanie centralnego „hubu" kryzysowego na bazie Centrum Koordynacji Reagowania Kryzysowego (ERCC), który byłby platformą współgrania międzysektorowego i budowania wspólnej świadomości sytuacyjnej,<br>- usprawnienie wykorzystania mechanizmu zintegrowanych uzgodnień UE dotyczącego reagowania na sytuacje kryzysowe na szczeblu politycznym (IPCR),<br>- wzmocnienie kooperacji i planowania cywilno-wojskowego, które mogłoby doprowadzić do powstania Europejskiego Mechanizmu Obrony Cywilnej,<br>- określenie konkretnych scenariuszy aktywowania klauzul wzajemnej pomocy i solidarności UE (art. 42.7 TUE i 222 TFUE)<br>• **zwiększenie świadomości sytuacyjnej i zdolności prognozowania:**<br>- poprawa zdolności gromadzenia i analizy informacji wywiadowczych na szczeblu unijnym,<br>- dostarczanie rządom państw członkowskich przez Centrum Satelitarne UE satelitarnych danych obserwacji Ziemi<br>• **wzmocnienie wymiany informacji i komunikacji:**<br>- terminowe wprowadzenie unijnego systemu łączności krytycznej (EUCCS) do 2030 r.,<br>- wspieranie wymiany informacji wrażliwych między grupą chętnych krajów UE, np. w domenie cyberbezpieczeństwa<br>• **wzmocnienie unijnej kultury ćwiczeń i szkoleń:**<br>- agregacja wniosków i lekcji z ćwiczeń w hubie wiedzy,<br>- wdrożenie międzysektorowych kursów szkoleniowych UE w obszarze bezpieczeństwa i gotowości |

| Obszar | Działania |
|---|---|
| **3. Zaangażowanie społeczne** | • **zwiększenie indywidualnej gotowości kryzysowej i gotowości gospodarstw domowych:**<br>- wprowadzanie tematów gotowości kryzysowej i odporności do programów edukacji w państwach członkowskich,<br>- promowanie wśród obywateli UE zasady utrzymywania indywidualnych zapasów kryzysowych na 72 godziny<br>• **usprawnienie powiadamiania mieszkańców o zagrożeniach**<br>• **zapobieganie podatności na kryzysy i katastrofy, w tym klęski żywiołowe**<br>• **promowanie aktywnej obywatelskości i przeciwdziałanie brakom kompetencyjno-kadrowym w sektorze bezpieczeństwa:**<br>- wypracowanie zachęt do podejmowania pracy w sektorze bezpieczeństwa narodowego (w tym w siłach zbrojnych) i ratowniczym przez młode osoby,<br>- wspieranie zaangażowania ochotniczego |
| **4. Partnerstwo publiczno-prywatne** | • **wzmocnienie współpracy publiczno-prywatnej w dziedzinie budowania odporności kryzysowej:**<br>- lepsza wymiana informacji pomiędzy administracją publiczną a sektorem prywatnym,<br>- przygotowanie klauzul kryzysowych w regulacjach UE z wykorzystaniem doświadczeń z doraźnych wyłączeń w zakresie państwowej pomocy czasu pandemii COVID-19,<br>- rozszerzenie i formalizacja współpracy kryzysowej sektora prywatnego z KE z wykorzystaniem doświadczeń z pandemii i kryzysu energetycznego,<br>- lepsze wykorzystanie doświadczeń sektora prywatnego w dziedzinie gotowości i planowania kryzysowego,<br>- włączenie zasady „gotowości z założenia" (*preparedness-by-design*) do rewizji Dyrektywy ws. Zamówień Publicznych w celu uproszczenia i przyspieszenia realizacji tychże w świetle obecnych wyzwań i zagrożeń<br>• **zwiększenie gotowości i odporności sektora prywatnego:**<br>- objęcie innych sektorów, w tym przemysłu zbrojeniowego, wymogami bezpieczeństwa infrastruktury krytycznej z dyrektyw CER (o odporności podmiotów krytycznych) i NIS (o środkach na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa),<br>- opracowanie oddzielnych wymogów dla newralgicznych firm (wytwórcy półprzewodników, branża lotniczo-kosmiczna, twórcy systemów komunikacyjnych, producenci maszyn i pojazdów), aby wzmocnić ich gotowość kryzysową i zdolność do przetrwania szoków,<br>- lepsza współpraca z sektorem prywatnym w celu ochrony infrastruktury krytycznej, np. podmorskich kabli i gazociągów<br>• opracowanie ***Europejskiej strategii rezerw strategicznych*** **(*EU Stockpiling Strategy*):**<br>- redukowanie zależności zewnętrznych,<br>- stworzenie listy kluczowych rezerw (np. żywność, surowce, sprzęt ratowniczy i medyczny) oraz zdefiniowanie ich minimalnych wymagań ilościowych,<br>- lepsze monitorowanie krytycznych elementów łańcucha dostaw, zdolności produkcyjnych oraz rezerw prywatnych,<br>- wypracowanie kryteriów uwalniania rezerw strategicznych oraz analiza możliwości wprowadzenia wspólnych zakupów na rzecz ich uzupełnienia |

| Obszar | Działania |
|---|---|
| **5. Zagrożenia hybrydowe** | • **wzmocnienie struktur wywiadowczych w UE, aby umożliwić zaawansowaną współpracę wywiadów:**<br>- wdrożenie postanowień *Kompasu strategicznego* w zakresie zdolności wywiadowczych,<br>- usprawnienie wymiany informacji między instytucjami unijnymi oraz zacieśnienie współpracy wywiadowczej państw członkowskich w ramach UE<br>• **wzmocnienie unijnego „odstraszania przez odmowę":**<br>- zachęcanie państw do wymiany informacji o zagrożeniach i współpracy kontrwywiadowczej,<br>- utworzenie unijnej sieci antysabotażowej bazującej na istniejących rozwiązaniach instytucjonalnych (Critical Entities Resilience Group, Protective Security Advisory Programme, Hybrid Fusion Cell, Frontex)<br>• **wzmocnienie unijnego „odstraszania przez karę":**<br>- przeprowadzenie kompleksowej analizy zagrożeń hybrydowych,<br>- wzmocnienie politycznego mechanizmu atrybucji ataku,<br>- wsparcie członków w walce z organizacjami terrorystycznymi, przestępczością zorganizowaną, aktami sabotażu i szpiegostwem poprzez stworzenie ram dostępu do informacji szyfrowanych |
| **6. Sektor zbrojeniowy** | • **wypracowanie unijnego pakietu zdolności obronnych na kolejną dekadę:**<br>- wykorzystanie *Białej księgi przyszłości europejskiej obronności* do wytyczenia ambitnych celów (m.in. zwiększenia finansowania wspólnotowego, ściślejszej współpracy z NATO, lepszego zarządzania sektorem obronnym),<br>- pełne wdrożenie *Europejskiej strategii przemysłowej w zakresie obronności* (EDIS),<br>- wybór flagowych projektów obronnych wspólnego zainteresowania (*Defence Projects of Common Interest*), którym zostanie zapewnione długofalowe finansowanie (za przykład niech posłużą obrona powietrzna i cybernetyczna, wymienione w wytycznych politycznych KE na lata 2024–2029),<br>- zapewnienie wystarczających środków na wspólne zakupy uzbrojenia i wspólne rozwijanie zdolności przez kraje unijne<br>• **wzmocnienie zdolności UE do wspierania militarnego Ukrainy:**<br>- zwiększanie mocy produkcyjnych przemysłu obronnego, aby móc rozszerzać pomoc dla Kijowa i uzupełniać potencjalne braki powstałe w wyniku ewentualnego ograniczenia dostaw uzbrojenia i sprzętu przez USA,<br>- zapewnienie odpowiedniego finansowania Europejskiemu Instrumentowi na rzecz Pokoju,<br>- wspieranie integracji Ukrainy z europejskim ekosystemem bezpieczeństwa<br>• **wprowadzenie jednolitego rynku przemysłu i usług zbrojeniowych**<br>• **zwiększenie inwestycji podwójnego zastosowania i wzmocnienie współpracy cywilno-wojskowej w duchu bezpieczeństwa całościowego:**<br>- tworzenie korytarzy mobilności wojskowej z infrastrukturą logistyczno-paliwową, magazynowanie rezerw strategicznych,<br>- ujednolicenie definicji „podwójnego zastosowania" w UE,<br>- zwiększenie nakładów na badania i rozwój w dziedzinie podwójnego zastosowania, w tym w technologie AI i kwantowe,<br>- rozwój programów bezpieczeństwa ludności z finansowaniem unijnym |

| Obszar | Działania |
|---|---|
| **7. Kontakty zewnętrzne i partnerstwa** | • **wdrożenie zasady wzajemnej odporności**<br>• **lepsze przygotowanie UE do reagowania na kryzysy w sąsiedztwie na podstawie ocen ryzyka i różnych scenariuszy:**<br>- wzmocnienie misji i operacji WPBiO, a także obecności morskiej w dziedzinie zabezpieczenia szlaków żeglugi i infrastruktury krytycznej (opcja wypracowania synergii instrumentów WPBiO i bezpieczeństwa wewnętrznego państw członkowskich w obszarach przygranicznych, w tym morskich przy wodach terytorialnych),<br>- wspomaganie państw i wspólnot wrażliwych na zmiany klimatu<br>• **zaangażowanie dyplomatyczne:**<br>- bardziej proaktywna dyplomacja UE,<br>- zwiększenie dostępności unijnych narzędzi wczesnego ostrzegania i wykrywania zagrożeń,<br>- wymiana z partnerami doświadczeń i praktyk w zakresie odporności, organizacja wspólnych szkoleń, rozważenie utworzenia centrów odporności (Mutual Resilience Centres)<br>• **analiza wspólnych interesów i możliwości współpracy z partnerami na rzecz budowania odporności**<br>• **zwiększenie zdolności planistycznych i przyspieszenie procesu decyzyjnego**<br>- zakorzenienie w planowaniu UE w zakresie strategii Global Gateway myślenia w kategoriach odporności i gotowości |
| **8. Aspekty budżetowe** | • **włączenie gotowości kryzysowej do budżetu UE i negocjacji WRF:**<br>- uelastycznienie WRF w celu zwiększenia zdolności szybkiego reagowania UE na kryzysy,<br>- uwzględnianie czynnika „wpływ na gotowość kryzysową" w ocenie inwestycji współfinansowanych z budżetu UE, w tym funduszy strukturalnych i regionalnych (w szczególności Funduszu Spójności), w postaci takich kategorii jak ryzyka czy odporność na katastrofy i zmiany klimatu,<br>- lepsze dostosowanie budżetu UE do wspierania wieloletnich inwestycji w gotowość kryzysową oraz zapewnienie odpowiednich środków na nie,<br>- zwiększenie inwestycji w infrastrukturę podwójnego zastosowania<br>• **stworzenie Ram Inwestycyjnych Europejskiej Gotowości Kryzysowej (European Preparedness and Readiness Investment Framework):**<br>- przygotowanie spójnego pakietu instrumentów finansowania gotowości kryzysowej w kolejnym cyklu budżetowym,<br>- wytyczenie celu dotyczącego wydatków na wzmacnianie gotowości kryzysowej w budżecie (np. 15%),<br>- rozważenie powołania dwóch instrumentów integrujących unijne inwestycje w bezpieczeństwo – Defending Europe Facility (przemysł zbrojeniowy) i Securing Europe Facility (ochrona ludności, bezpieczeństwo granic, reagowanie kryzysowe, ochrona infrastruktury krytycznej),<br>- powołanie inwestycyjnego programu gwarancyjnego (Investment Guarantee Programme), który mógłby być wzorowany na InvestEU i motywować sektor prywatny do inwestycji w obronność (przemysł i technologie) oraz gotowość kryzysową,<br>- współpraca z Europejskim Bankiem Inwestycyjnym na rzecz pobudzenia sektora obronnego także poza kategorią podwójnego zastosowania |