Rada
Unii Europejskiej

Bruksela, 3 kwietnia 2025 r.
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	2 kwietnia 2025 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2025) 148 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego

Delegacje otrzymują w załączeniu dokument COM(2025) 148 final.

Zał.: COM(2025) 148 final

KOMISJA
EUROPEJSKA

Strasburg, dnia 1.4.2025 r.
COM(2025) 148 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

w sprawie ProtectEU: europejska strategia bezpieczeństwa wewnętrznego

1. ProtectEU: europejska strategia bezpieczeństwa wewnętrznego

Bezpieczeństwo jest fundamentem, na którym opierają się wszystkie nasze wolności. Demokracja, praworządność, prawa podstawowe, dobrobyt Europejczyków, konkurencyjność i dostatek – wszystko to zależy od zdolności Unii do zapewnienia podstawowej gwarancji bezpieczeństwa. W nowej erze zagrożeń bezpieczeństwa, w której obecnie żyjemy, zdolność państw członkowskich UE do zagwarantowania bezpieczeństwa swoim obywatelom jest bardziej niż kiedykolwiek uwarunkowana przyjęciem **jednolitego europejskiego podejścia do ochrony naszego bezpieczeństwa wewnętrznego**. W zmieniającej się sytuacji geopolitycznej Europa musi nadal wywiązywać się ze złożonej obietnicy zapewnienia pokoju.

Podjęto już pierwsze kroki w kierunku budowy europejskiego aparatu bezpieczeństwa. W ostatnim dziesięcioleciu wyposażyliśmy Unię w ulepszone zbiorowe mechanizmy działania w obszarach egzekwowania prawa i współpracy sądowej, bezpieczeństwa granic, zwalczania poważnej i zorganizowanej przestępczości, przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi oraz ochrony fizycznej i cyfrowej infrastruktury krytycznej UE. Kluczowe znaczenie ma właściwe wdrożenie uprzednio przyjętych przepisów i opracowanych strategii politycznych.

Ze względu na charakter obecnych zagrożeń i nierozerwalny związek między bezpieczeństwem wewnętrznym i zewnętrznym UE musimy podjąć szerzej zakrojone działania.

Krajobraz zagrożeń jest niepokojący. Zacierają się granice między **zagrożeniami hybrydowymi** a otwartą wojną. Rosja prowadzi kampanię hybrydową online i offline przeciwko UE i jej partnerom, aby zakłócić i podważyć spójność społeczną i procesy demokratyczne oraz przetestować solidarność UE z Ukrainą. Wrogie państwa obce i podmioty sponsorowane przez państwo starają się infiltrować i zakłócać naszą infrastrukturę krytyczną i łańcuchy dostaw, wykradać dane wrażliwe, przygotowując się do maksymalnego zakłócania w przyszłości. Wykorzystują one przestępczość jako narzędzie, a przestępców – jako popleczników. Ponadto nasza zależność od państw trzecich pod względem łańcuchów dostaw sprawia, że jesteśmy bardziej podatni na kampanie hybrydowe prowadzone przez wrogie państwa.

Silne **sieci przestępczości zorganizowanej** rozprzestrzeniają się w Europie, rozwijają się w internecie, przenikają do naszej gospodarki i wpływają na nasze społeczeństwo, co podkreślono w niedawno przedstawionej przez Europol ocenie zagrożenia poważną i zorganizowaną przestępczością w UE (SOCTA)[1]. Gdy przestępczość zorganizowana zdobędzie przyczółek w danej społeczności lub sektorze gospodarki, jej wyeliminowanie staje się trudną walką: jedna trzecia najgroźniejszych siatek przestępczych działa od ponad dziesięciu lat. W praniu pieniędzy i ukrywaniu korzyści pochodzących z przestępstwa pomagają im kryptowaluty i równoległe systemy finansowe.

Poziom zagrożenia terrorystycznego w Europie nadal rośnie. Kryzysy regionalne poza UE wywołują efekt domina, dając podmiotom terrorystycznym z całego spektrum ideologicznego nową motywację do werbowania, mobilizacji lub budowania swoich zdolności. Ich działania w zakresie radykalizacji i werbowania skierowane są w szczególności do najsłabszych grup naszych społeczeństw, a zwłaszcza do niektórych osób młodych. Podżegają do ataków w pojedynkę i powodują gwałtowny wzrost ekstremizmu antysystemowego, którego celem jest zakłócenie demokratycznego porządku prawnego.

Szybki **postęp technologiczny** zapewnia niezbędne narzędzia służące wzmocnieniu unijnego aparatu bezpieczeństwa. Jednak cyberataki i obca manipulacja informacją stają się coraz

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

powszechniejsze i ich sprawcy wykorzystują nowe technologie, takie jak sztuczna inteligencja. Szczególnie narażone na zagrożenia w sieci są dzieci, młodzież i osoby starsze, a rozprzestrzenianie się nienawiści w internecie zagraża wolności wypowiedzi i spójności społecznej.

Nasze życie stało się mniej bezpieczne i ten stan rzeczy jest coraz bardziej odczuwalny przez Europejczyków, których **poczucie bezpieczeństwa i ochrony w UE** osłabło do tego stopnia, że na pytanie o przyszłość 64 % respondentów wyraziło obawę o bezpieczeństwo UE[2]. W coraz większym stopniu zaniepokojeni są również przedsiębiorcy; wśród dziesięciu największych zagrożeń wskazanych w sprawozdaniu Światowego Forum Ekonomicznego dotyczącym globalnych zagrożeń z 2025 r.[3] znalazły się informacje wprowadzające w błąd i dezinformacja, przestępczość i nielegalna działalność oraz cyberszpiegostwo.

Europejczycy powinni **móc prowadzić życie wolne od strachu** – na ulicach, w domu, w miejscach publicznych, w metrze czy w internecie. Ochrona ludzi, zwłaszcza najbardziej narażonych na ataki, które w nieproporcjonalny sposób dotykają dzieci, kobiety i mniejszości, w tym społeczności żydowskie i muzułmańskie, jest najważniejszym elementem działań UE na rzecz bezpieczeństwa. Ma ona zasadnicze znaczenie dla budowania odpornych i spójnych społeczeństw.

Komisja opracowuje **europejską strategię bezpieczeństwa wewnętrznego**, aby lepiej przeciwdziałać zagrożeniom w nadchodzących latach. Dzięki bardziej precyzyjnemu zestawowi narzędzi prawnych, zacieśnieniu współpracy i intensywniejszej wymianie informacji Unia zwiększy swoją odporność i wspólną zdolność do przewidywania zagrożeń bezpieczeństwa, zapobiegania im, wykrywania ich i skutecznego reagowania na nie. Jednolite podejście do bezpieczeństwa wewnętrznego może pomóc państwom członkowskim w wykorzystaniu potęgi technologii do wzmacniania, a nie osłabiania bezpieczeństwa, przy jednoczesnym promowaniu bezpiecznej przestrzeni cyfrowej dla wszystkich. Podejście to wspiera ponadto wspólną reakcję państw członkowskich na globalne zmiany polityczne i gospodarcze, które mają wpływ na bezpieczeństwo wewnętrzne Unii.

Niniejsza strategia opiera się na **trzech zasadach**, a jej rdzeniem jest poszanowanie praworządności i praw podstawowych.

Po pierwsze, określono w niej ambitny cel zmiany kultury w dziedzinie bezpieczeństwa. Unia potrzebuje **podejścia obejmującego całe społeczeństwo**, angażującego wszystkich obywateli i zainteresowane strony, w tym społeczeństwo obywatelskie, ośrodki badawcze, środowisko akademickie i podmioty prywatne. Działania w ramach strategii opierają się zatem w miarę możliwości na zintegrowanym podejściu z udziałem wielu zainteresowanych stron.

Po drugie, **względy bezpieczeństwa należy zintegrować ze wszystkimi przepisami, politykami i programami UE**, w tym działaniami zewnętrznymi UE, i włączyć je do ich głównego nurtu. Prawodawstwo, polityki i programy trzeba będzie przygotowywać, poddawać przeglądom i wdrażać z uwzględnieniem perspektywy bezpieczeństwa, upewniając się, że zajęto się niezbędnymi względami bezpieczeństwa, aby promować spójne i kompleksowe podejście do bezpieczeństwa.

Co więcej, bezpieczna, chroniona i odporna Europa wymaga **poważnych inwestycji ze strony UE, jej państw członkowskich i sektora prywatnego**. Priorytety i działania określone w niniejszej strategii wymagają wystarczających zasobów ludzkich i finansowych, aby zapewnić ich realizację. Jak określono w komunikacie pt. „Droga ku następnym wieloletnim

[2] Badanie Eurobarometr Flash FL550: Wyzwania i priorytety UE.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, s.17.

ramom finansowym”[4], Europa będzie musiała zwiększyć wydatki publiczne na bezpieczeństwo oraz promować badania i inwestycje w dziedzinie bezpieczeństwa, zwiększając swoją autonomię strategiczną.

Niniejsza strategia uzupełnia **strategię na rzecz unii gotowości**[5], w której określono zintegrowane podejście uwzględniające wszystkie zagrożenia w zakresie gotowości na wypadek konfliktów, katastrof spowodowanych przez człowieka i klęsk żywiołowych oraz kryzysów, a także **białą księgę w sprawie obronności europejskiej – Gotowość 2030**[6], która wspiera rozwój i nabywanie zdolności obronnych w całej UE w celu odstraszania zagranicznych przeciwników. Komisja zaproponuje również **europejską tarczę demokracji** w celu wzmocnienia odporności demokratycznej w UE. Razem w tych inicjatywach przedstawiono wizję bezpiecznej, chronionej i odpornej UE.

Nowe zarządzanie bezpieczeństwem wewnętrznym w Europie

Komisja będzie ściśle współpracować z państwami członkowskimi i agencjami UE w celu ulepszenia podejścia UE do bezpieczeństwa wewnętrznego zarówno na szczeblu strategicznym, jak i operacyjnym.

Cel ten zostanie osiągnięty przez:

- **konsekwentne określanie potencjalnego wpływu nowych i zmienionych inicjatyw Komisji na bezpieczeństwo i gotowość od samego początku i przez cały czas trwania procesu negocjacji;**
- **regularne spotkania działającej w ramach Komisji grupy projektowej ds. europejskiego bezpieczeństwa wewnętrznego, wspierane przez strategiczną współpracę międzysektorową w całej Komisji;**
- **przedstawianie analiz zagrożeń związanych z bezpieczeństwem wewnętrznym w celu wsparcia prac Kolegium Bezpieczeństwa;**
- **dyskusje z państwami członkowskimi w Radzie na temat zmieniających się zagrożeń bezpieczeństwa wewnętrznego w oparciu o analizę zagrożeń i wymianę informacji na temat kluczowych priorytetów politycznych;**
- **przedkładanie regularnych sprawozdań Parlamentowi Europejskiemu i Radzie w celu śledzenia i wspierania systematycznego wdrażania kluczowych inicjatyw w zakresie bezpieczeństwa.**

2. Zintegrowana orientacja sytuacyjna i analiza zagrożeń

Zapewnimy UE nowe sposoby wymiany i łączenia informacji oraz regularną analizę zagrożeń bezpieczeństwa wewnętrznego UE, co przyczyni się do kompleksowej oceny ryzyka i zagrożeń.

Bezpieczeństwo zaczyna się od **skutecznego przewidywania**. UE musi polegać na kompleksowej, wystarczająco autonomicznej i aktualnej orientacji sytuacyjnej oraz analizie zagrożeń. Użyteczne operacyjnie dane wywiadowcze, do których dalszego wzmacniania zachęca się państwa członkowskie za pośrednictwem pojedynczej komórki analiz wywiadowczych (SIAC), będącej pojedynczym punktem kontaktowym dla danych wywiadowczych państw członkowskich, mają zasadnicze znaczenie dla oceny zagrożeń

[4] COM(2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

i przeciwdziałania im, co ostatecznie stanowi podstawę działań politycznych i legislacyjnych[7]. Musimy wykorzystywać **analizy oparte na danych wywiadowczych** i **oceny zagrożeń** na szczeblu UE w sposób bardziej skuteczny i oparty na współpracy.

Opierając się na poszczególnych ocenach ryzyka i zagrożeń sporządzanych na szczeblu UE i w odniesieniu do poszczególnych sektorów[8], Komisja będzie przygotowywać **regularne unijne analizy zagrożeń bezpieczeństwa wewnętrznego** w celu identyfikacji głównych wyzwań w zakresie bezpieczeństwa, z myślą o określeniu priorytetów politycznych. Pomogą one opracować sprawną i elastyczną politykę bezpieczeństwa wewnętrznego, która skutecznie reaguje na zmieniające się zagrożenia, lepiej chroni ludzi i przedsiębiorstwa przed atakami oraz umożliwia ukierunkowane interwencje polityczne w odpowiednim czasie. Te unijne analizy zagrożeń bezpieczeństwa wewnętrznego przyczynią się również do **kompleksowej (międzysektorowej, uwzględniającej wszystkie zagrożenia) unijnej oceny ryzyka i zagrożeń** opracowanej przez Komisję i wysoką przedstawicielkę, jak określono w strategii na rzecz unii gotowości.

Zasadnicze znaczenie dla wymiany informacji ma zaufanie i bezpieczne postępowanie z nimi, a to wymaga niezawodnej i bezpiecznej infrastruktury. Instytucje, organy, urzędy i agencje Unii muszą zapewnić sobie możliwość korzystania z **bezpiecznych kanałów komunikacji** w celu wymiany informacji szczególnie chronionych i niejawnych między sobą oraz z państwami członkowskimi. Inwestycje w **interoperacyjne bezpieczne systemy** i niezawodne technologie wzmocnią autonomię UE i zwiększą jej zdolność do zarządzania kryzysami i zapewnienia odporności operacyjnej. W tym kontekście Komisja wzywa współprawodawców do zakończenia negocjacji w sprawie **proponowanego rozporządzenia w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii**, w szczególności w celu zapewnienia wspólnych ram postępowania ze szczególnie chronionymi informacjami jawnymi i niejawnymi[9].

Dla zapewnienia własnego bezpieczeństwa operacyjnego i orientacji sytuacyjnej Komisja dokona przeglądu swoich korporacyjnych ram zarządzania w zakresie bezpieczeństwa i ustanowi **zintegrowane centrum monitorowania bezpieczeństwa (ISOC)**, aby chronić ludzi, aktywa fizyczne i operacje we wszystkich obiektach Komisji. Komisja zwiększy również swoje zdolności operacyjne i analityczne w zakresie identyfikowania i łagodzenia zagrożeń hybrydowych.

Zgodnie ze strategią na rzecz unii gotowości kwestie gotowości i względy bezpieczeństwa zostaną połączone i włączone do głównego nurtu prawodawstwa, polityk i programów UE. Przygotowując przepisy, polityki lub programy z uwzględnieniem perspektywy gotowości i bezpieczeństwa lub dokonując ich przeglądu, Komisja będzie konsekwentnie określać potencjalny wpływ preferowanego wariantu polityki na gotowość i bezpieczeństwo. Decydentom politycznym w Komisji proponowane będą regularne szkolenia.

Aby wesprzeć państwa członkowskie, Komisja omówi z Radą zmieniające się zagrożenia bezpieczeństwa wewnętrznego i kluczowe priorytety polityczne oraz będzie regularnie informować o realizacji strategii. Ponadto Komisja będzie na bieżąco informować Parlament

[7] Safer together – Strengthening Europe's Civilian and Military Preparedness and Readiness [Razem bezpieczniej – Wzmocnienie gotowości cywilnej i wojskowej Europy], s. 23.

[8] Sektorowe oceny zagrożeń, które będą stanowić podstawę tej analizy zagrożeń, obejmują ocenę zagrożenia poważną i zorganizowaną przestępczością w UE (SOCTA), sprawozdanie dotyczące sytuacji i tendencji w dziedzinie terroryzmu w UE, wspólne sprawozdanie z oceny cyberbezpieczeństwa (JCAR) oraz przyszłe oceny zagrożeń, ryzyka i metod prania pieniędzy i finansowania terroryzmu, które mają zostać przeprowadzone przez Komisję i Urząd ds. Przeciwdziałania Praniu Pieniędzy.

[9] COM(2022) 119 final.

Europejski i odpowiednie zainteresowane strony oraz angażować się we wszystkie stosowne działania.

Kluczowe działania

Komisja:

- **będzie opracowywać i przedstawiać regularne analizy zagrożeń bezpieczeństwa wewnętrznego UE.**

Państwa członkowskie wzywa się do:

- **usprawnienia wymiany danych wywiadowczych z SIAC i zapewnienia lepszej wymiany informacji z agencjami i organami UE.**

Parlament Europejski i Radę zachęca się do:

- **zakończenia negocjacji w sprawie proponowanego rozporządzenia w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii.**

3. Wzmocnione zdolności UE w zakresie bezpieczeństwa

Opracujemy nowe narzędzia egzekwowania prawa, takie jak zmodernizowany Europol, oraz lepsze środki koordynacji i zapewnienia bezpiecznej wymiany danych i zgodnego z prawem dostępu do danych.

Aby skutecznie przeciwdziałać zmieniającym się zagrożeniom, UE musi zwiększyć swoje zdolności w zakresie bezpieczeństwa i wspierać innowacje. Organy ścigania i organy sądowe – będące głównymi podmiotami przeciwdziałającym zagrożeniom bezpieczeństwa wewnętrznego – potrzebują odpowiednich narzędzi i zdolności operacyjnych do szybkiego i skutecznego działania. Ważne jest, aby organy te były w stanie komunikować się i koordynować działania ponad granicami i między służbami w celu skutecznego zapobiegania, wykrywania, prowadzenia dochodzeń i ścigania.

Agencje i organy UE ds. bezpieczeństwa wewnętrznego

Agencje i organy UE zajmujące się wymiarem sprawiedliwości, sprawami wewnętrznymi i cyberbezpieczeństwem odgrywają kluczową rolę w architekturze bezpieczeństwa UE – rolę, która stale rośnie wraz z rozszerzaniem się ich obowiązków.

Dziś – 25 lat od jego utworzenia – **Europol** ma większe niż kiedykolwiek znaczenie dla unijnych ram bezpieczeństwa. Wspiera on złożone dochodzenia transgraniczne, ułatwia wymianę informacji, opracowuje innowacyjne narzędzia dla policji i zapewnia zaawansowaną wiedzę fachową na potrzeby organów ścigania. Szereg czynników uniemożliwia jednak Europolowi pełne wykorzystanie jego potencjału operacyjnego we wspieraniu działań dochodzeniowych i operacyjnych mających na celu zwalczanie przestępczości transgranicznej: należą do nich zarówno niewystarczające zasoby, jak i fakt, że jego obecny mandat nie obejmuje nowych zagrożeń bezpieczeństwa, takich jak sabotaż, zagrożenia hybrydowe lub manipulacja informacją. Dlatego też Komisja zaproponuje **ambitny przegląd mandatu Europolu**, aby przekształcić go w prawdziwie operacyjną agencję policyjną, lepiej wspierającą państwa członkowskie. Celem jest rozwijanie technologicznej wiedzy specjalistycznej i zdolności Europolu do wspierania krajowych organów ścigania, poprawa koordynacji z innymi agencjami i organami oraz z państwami członkowskimi, wzmocnienie partnerstw strategicznych z krajami partnerskimi i sektorem prywatnym oraz zapewnienie wzmocnionego nadzoru nad Europolem.

Ponadto Komisja będzie dążyć do dalszej **poprawy skuteczności i komplementarności agencji i organów UE zajmujących się bezpieczeństwem wewnętrznym oraz do wzmocnienia sprawnej współpracy** między nimi.

Mandat **Eurojustu** zostanie poddany ocenie i wzmocniony w celu zwiększenia skuteczności współpracy sądowej, zwiększenia komplementarności i współpracy z Europolem. Obejmie to zwiększenie skuteczności Eurojustu, a także jego zdolności do zapewniania proaktywnego wsparcia i analiz organom sądowym państw członkowskich. Ponadto, biorąc pod uwagę wyjątkowe kompetencje **EPPO** w zakresie prowadzenia śledztw i ścigania przestępstw naruszających interesy finansowe Unii, Komisja rozważy najlepsze sposoby poprawy zdolności EPPO do ochrony środków finansowych Unii. Obejmie to zacieśnienie współpracy między EPPO a Europolem.

Kluczowe znaczenie dla współpracy ma **skuteczna i bezpieczna wymiana informacji między agencjami**. Europol i Frontex potrzebują szybkiej wzajemnej wymiany informacji, w tym do celów operacyjnych, jak wynika ze wspólnego oświadczenia ze stycznia 2024 r.[10] Centralną rolę w zapewnianiu bezpiecznego przechowywania i dostępności danych w celu lepszej koordynacji i skuteczniejszej wymiany informacji między agencjami odgrywa **eu-LISA**. Wiedzę fachową w zakresie ochrony praw podstawowych przy opracowywaniu i wdrażaniu polityki bezpieczeństwa zapewnia **Agencja Praw Podstawowych Unii Europejskiej**.

Unijny Urząd ds. Przeciwdziałania Praniu Pieniędzy (AMLA) został uprawniony do krzyżowego porównywania informacji na zasadzie trafienia/braku trafienia z informacjami udostępnionymi przez Europol, EPPO, Eurojust i Europejski Urząd ds. Zwalczania Nadużyć Finansowych w celu przeprowadzania wspólnych analiz spraw transgranicznych.

Kluczową rolę we wdrażaniu europejskich przepisów dotyczących cyberbezpieczeństwa odgrywa **ENISA**. W ramach zbliżającego się **przeglądu aktu o cyberbezpieczeństwie** Komisja oceni jej mandat i zaproponuje jego modernizację w celu zwiększenia unijnej wartości dodanej.

Współpraca między organami celnymi a innymi organami ścigania zostanie zacieśniona dzięki proponowanemu utworzeniu **Urzędu UE ds. Celnych** i **unijnego centrum danych celnych** w ramach pakietu reform celnych UE. Informacje z przyszłego centrum i powiązane dane z Europolu, Eurojustu, EPPO, OLAF-u, AMLA i Fronteksu, w ramach ich odpowiednich kompetencji, ulepszą wspólną analizę i przyczynią się do bardziej spójnych działań operacyjnych, w szczególności na granicach zewnętrznych. Komisja zachęca współprawodawców do szybkiego zakończenia negocjacji w sprawie reformy celnej UE i będzie nadal wspierać ich w tym zakresie.

Zwiększenie komplementarności między EPPO, OLAF-em, Europolem, Eurojustem, AMLA i proponowanym Urzędem UE ds. Celnych będzie również opierać się na wynikach trwającego przeglądu **unijnej struktury zwalczania nadużyć finansowych**. To całościowe podejście może przynieść korzyści w zakresie bezpieczeństwa wewnętrznego, ponieważ koncentruje się na lepszym wykorzystaniu zarówno środków karnych, jak i administracyjnych, interoperacyjności systemów informatycznych i lepszej współpracy.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Łączność krytyczna

Obecnie **systemy łączności krytycznej**[11] działają w większości przypadków oddzielnie na szczeblu krajowym. Oznacza to, że służby interwencyjne często nie mogą komunikować się ze swoimi odpowiednikami przy przekraczaniu granicy z innymi państwami członkowskimi. W niektórych państwach członkowskich istnieją również ograniczenia w komunikacji między różnymi rodzajami służb interwencyjnych (np. policją i karetkami pogotowia). Standardy większości systemów nie spełniają obecnych wymogów w zakresie funkcjonalności i odporności, co znacznie ogranicza zdolność reagowania służb interwencyjnych, zwłaszcza w wymiarze transgranicznym.

Aby zwiększyć zdolność UE do reagowania na sytuacje kryzysowe, Komisja zaproponuje przepisy mające na celu utworzenie **europejskiego systemu łączności krytycznej (EUCCS)** łączącego systemy łączności krytycznej nowej generacji państw członkowskich w UE. Celem jest, aby EUCCS opierał się na trzech filarach strategicznych: mobilności operacyjnej, dużej odporności i autonomii strategicznej. Inicjatywa EUCCS określi zharmonizowane wymogi i pomoże zmodernizować systemy łączności krytycznej państw członkowskich, umożliwiając im sprawne funkcjonowanie. Rozszerzy również zasięg systemu dzięki przyszłemu wieloorbitalnemu systemowi IRIS[2][12]. Projekty finansowane przez UE pomogą rozwijać zdolności techniczne EUCCS, opierając się przede wszystkim na europejskich dostawcach technologii, aby wspierać autonomię strategiczną UE w tym wrażliwym sektorze.

Zgodny z prawem dostęp do danych

Organy ścigania i organy sądowe muszą mieć możliwość prowadzenia dochodzeń i podejmowania działań przeciwko przestępczości. Obecnie prawie wszystkie formy poważnej i zorganizowanej przestępczości mają swój ślad cyfrowy[13]. Około 85 % postępowań przygotowawczych opiera się obecnie na zdolności organów ścigania do uzyskiwania dostępu do informacji cyfrowych[14].

Grupa wysokiego szczebla ds. dostępu do danych do celów skutecznego egzekwowania prawa podkreśliła w swoim sprawozdaniu końcowym[15], że na przestrzeni ostatnich dziesięciu lat organy ścigania i wymiar sprawiedliwości przegrywały z przestępcami, ponieważ przestępcy wykorzystują narzędzia i produkty dostarczane z innych jurysdykcji przez dostawców, którzy wprowadzili środki pozbawiające ich możliwości współpracy w przypadku zgodnych z prawem wniosków w indywidualnych sprawach karnych. Systematyczna współpraca między organami ścigania a podmiotami prywatnymi, w tym dostawcami usług, ma zatem zasadnicze znaczenie w przyszłych wysiłkach na rzecz rozbicia najgroźniejszych siatek przestępczych i walki z przestępcami w Unii i poza nią.

W miarę jak cyfryzacja staje się coraz bardziej powszechna i przestępcy zyskują dostęp do rosnącej liczby nowych narzędzi, zasadnicze znaczenie mają ramy dostępu do danych odpowiadające potrzebom egzekwowania naszych praw i ochrony naszych wartości.

[11] Są nimi sieci wykorzystywane przez organy ścigania, straż graniczną, organy celne, ochronę ludności, straż pożarną, ratownictwo medyczne i inne kluczowe podmioty odpowiedzialne za bezpieczeństwo publiczne i ochronę publiczną.

[12] Unijna infrastruktura na rzecz odporności, wzajemnych połączeń i bezpieczeństwa za pośrednictwem satelitów.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[14] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52019PC0070.

[15] Concluding report of the High-Level Group on access to data for effective law enforcement [Sprawozdanie końcowe grupy wysokiego szczebla ds. dostępu do danych do celów skutecznego egzekwowania prawa], 15 listopada 2024 r., 4802e306-c364-4154-835b-e986a9a49281_en.

Jednocześnie dbałość o zabezpieczenie systemów cyfrowych przed nieuprawnionym dostępem ma równie istotne znaczenie dla zachowania cyberbezpieczeństwa i ochrony przed pojawiającymi się zagrożeniami bezpieczeństwa. Takie ramy dostępu muszą również być zgodne z prawami podstawowymi, zapewniając m.in. odpowiednią ochronę prywatności i danych osobowych.

W ostatnich latach UE podjęła działania zarówno w celu zwalczania **przestępczości internetowej, jak i ułatwienia dostępu do dowodów cyfrowych w przypadku wszystkich przestępstw**, przyjmując przepisy dotyczące elektronicznego materiału dowodowego, które będą w pełni obowiązywać od sierpnia 2026 r.[16] Ich uzupełnieniem będą międzynarodowe instrumenty wymiany informacji i dowodów. Komisja zaproponuje wkrótce podpisanie i zawarcie nowej **konwencji ONZ przeciwko cyberprzestępczości**.

Aby podjąć działania następcze w związku z zaleceniami grupy wysokiego szczebla[17], w pierwszej połowie 2025 r. Komisja przedstawi **plan działania określający prawne i praktyczne środki**, które proponuje wdrożyć **w celu zapewnienia uprawnionego i skutecznego dostępu do danych**. W ramach działań następczych w związku z tym planem działania Komisja priorytetowo potraktuje ocenę wpływu **przepisów dotyczących zatrzymywania danych** na szczeblu UE oraz przygotowanie **planu działania w zakresie technologii dotyczącego szyfrowania**, aby wskazać i ocenić rozwiązania technologiczne, które umożliwiłyby organom ścigania dostęp do zaszyfrowanych danych w sposób zgodny z prawem, chroniąc cyberbezpieczeństwo i prawa podstawowe.

Współpraca operacyjna

Komisja będzie współpracować z państwami członkowskimi, agencjami i organami UE oraz krajami partnerskimi w celu wzmocnienia współpracy operacyjnej, która ma zasadnicze znaczenie dla skuteczniejszego podejścia do zwalczania międzynarodowej przestępczości zorganizowanej i terroryzmu.

Europejska multidyscyplinarna platforma przeciwko zagrożeniom przestępstwami (EMPACT), która stanowi główne unijne ramy wspólnych działań przeciwko poważnej i zorganizowanej przestępczości, osiągnęła znaczące wyniki operacyjne. Kolejny cykl EMPACT na lata 2026–2029 stanowi okazję do dalszego wzmocnienia tych ram. Aby rozbijać najgroźniejsze siatki przestępcze i podejmować działania przeciwko przestępcom, Unia musi usprawnić i skoncentrować swoje wysiłki na najpilniejszych priorytetach, zwiększając zobowiązania państw członkowskich i zapewniając skuteczne wykorzystanie zasobów.

W tym celu Komisja będzie współpracować z prezydencjami Rady i państwami członkowskimi, aby **zmaksymalizować potencjał EMPACT i zająć się kluczowymi priorytetami kolejnego cyklu EMPACT na lata 2026–2029.** W tych obszarach priorytetowych potrzebne są dane wywiadowcze dotyczące najgroźniejszych siatek przestępczych, wspólne dochodzenia i operacyjne grupy zadaniowe oraz zdecydowana reakcja wymiaru sprawiedliwości, w tym zasada podążania śladem pieniędzy. Ponadto Unia musi zająć się kwestią werbowania przestępców i infiltracji przestępczej oraz zintensyfikować współpracę pomiędzy wieloma agencjami i organami ścigania w zakresie spraw międzynarodowych oraz odnośne szkolenia.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności, Dz.U. L 191 z 28.7.2023.

[17] Konkluzje Rady w sprawie dostępu do danych do celów skutecznego egzekwowania prawa (12 grudnia 2024 r.) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/pl/pdf.

Komisja będzie również wspierać inne formy **transgranicznej współpracy operacyjnej organów ścigania między państwami członkowskimi i państwami stowarzyszonymi w ramach Schengen**. Strefa Schengen, bez kontroli na granicach wewnętrznych, wymaga ścisłej współpracy i wymiany informacji między organami ścigania państw członkowskich w celu zapewnienia wysokiego poziomu bezpieczeństwa wewnętrznego. Obecnie funkcjonariusze organów ścigania nadal napotykają wyzwania podczas inwigilacji lub przeprowadzania pilnych interwencji transgranicznych[18], a przeciwdziałanie zagrożeniom hybrydowym wymaga również ściślejszej współpracy transgranicznej. Należy utworzyć **grupę wysokiego szczebla ds. przyszłości współpracy operacyjnej organów ścigania**, która opracuje wspólną wizję strategiczną.

Zasadnicze znaczenie dla skutecznej współpracy transgranicznej ma również skuteczna wymiana danych między organami ścigania. **Architektura interoperacyjności**, gdy zostanie utworzona, zapewni organom ścigania i Europolowi skuteczny dostęp do kluczowych informacji. Jednocześnie UE i jej państwa członkowskie powinny priorytetowo traktować dwustronną i wielostronną wymianę informacji poprzez prawne i techniczne wdrożenie **rozporządzenia Prüm II**[19], we współpracy z eu-LISA i Europolem. Umożliwi to bezpieczną zautomatyzowaną wymianę odcisków palców, profili DNA, danych rejestracyjnych pojazdów, wizerunków twarzy i informacji z rejestrów policyjnych za pośrednictwem routerów UE. Na szczeblu krajowym państwa członkowskie muszą wdrożyć **dyrektywę w sprawie wymiany informacji**[20] usprawniającą kanały wymiany informacji w celu sprawnego transgranicznego przepływu informacji, przy jednoczesnym zapewnieniu ich integracji z systemami na szczeblu Unii, takimi jak SIENA[21].

Skuteczna współpraca transgraniczna opiera się również na wspieraniu **wspólnej kultury egzekwowania prawa Unii**. Zasadnicze znaczenie dla osiągnięcia tego celu mają wspólne szkolenia, centra doskonałości i programy mobilności. Komisja zbada, w jaki sposób UE może najlepiej wspierać szkolenia dla organów państw członkowskich, polegając na **CEPOL-u** jako agencji UE ds. szkolenia w dziedzinie ścigania.

Poprawa bezpieczeństwa granic

Poprawa odporności i bezpieczeństwa granic zewnętrznych ma kluczowe znaczenie dla przeciwdziałania zagrożeniom hybrydowym, takim jak wykorzystywanie migracji jako broni, dla zapobiegania przedostawaniu się do UE podmiotów i towarów stwarzających zagrożenie oraz dla skutecznego zwalczania przestępczości transgranicznej i terroryzmu. W 2026 r. **planuje się udoskonalenie Systemu Informacyjnego Schengen (SIS)**, aby umożliwić państwom członkowskim wprowadzanie ostrzeżeń dotyczących obywateli państw trzecich zaangażowanych w terroryzm, w tym zagranicznych bojowników terrorystycznych, oraz w inne poważne przestępstwa, na podstawie danych udostępnianych Europolowi przez państwa trzecie.

[18] Zgodnie z przedstawioną przez Komisję oceną skutków wykonania przez państwa członkowskie zalecenia Rady (UE) 2022/915 z dnia 9 czerwca 2022 r. w sprawie współpracy operacyjnej organów ścigania (5909/25).

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/982 z dnia 13 marca 2024 r. w sprawie zautomatyzowanego przeszukania danych i zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej oraz zmieniające decyzje Rady 2008/615/WSiSW i 2008/616/WSiSW oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1726, (UE) 2019/817 i (UE) 2019/818 (rozporządzenie Prüm II), Dz.U. L, 2024/982, 5.4.2024.

[20] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/977 z dnia 10 maja 2023 r. w sprawie wymiany informacji między organami ścigania państw członkowskich i uchylająca decyzję ramową Rady 2006/960/WSiSW, Dz.U. L 134 z 22.5.2023, s. 1.

[21] Aplikacja sieci bezpiecznej wymiany informacji.

Dzięki lepszej **interoperacyjności** wielkoskalowych systemów informacyjnych UE państwa członkowskie uzyskają istotne informacje na temat osób z państw trzecich przekraczających lub zamierzających przekroczyć granice zewnętrzne, co pomoże organom ocenić warunki zezwolenia na wjazd na terytorium państw członkowskich[22]. Komisja będzie nadal ściśle współpracować z państwami członkowskimi i eu-LISA w celu szybkiego wdrożenia tych systemów, w szczególności **systemu wjazdu/wyjazdu (EES), europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmienionego wizowego systemu informacyjnego (VIS)**, aby zapewnić ich sprawne funkcjonowanie i korzyści w zakresie bezpieczeństwa.

Aby jeszcze bardziej zwiększyć bezpieczeństwo granic i zacieśnić współpracę UE w obliczu zmieniających się zagrożeń, **Komisja zaproponuje wzmocnienie zdolności Fronteksu.** Liczba funkcjonariuszy Europejskiej Straży Granicznej i Przybrzeżnej powinna z czasem wzrosnąć trzykrotnie do 30 000. Agencja ta powinna dysponować zaawansowaną technologią nadzoru i orientacji sytuacyjnej, w tym danymi wywiadowczymi istotnymi dla europejskiego zintegrowanego zarządzania granicami, oraz posiadać dostęp do solidnego unijnego programu obserwacji Ziemi w ramach usługi rządowej na potrzeby kontroli granicznej, który ma zostać uruchomiony do 2027 r. Działania te powinny jeszcze bardziej zwiększyć zdolność do wykrywania przestępczości transgranicznej na granicach zewnętrznych, zapobiegania jej i jej zwalczania, a także zwiększyć wsparcie udzielane państwom członkowskim w realizacji powrotów, w szczególności w odniesieniu do obywateli państw trzecich stwarzających zagrożenie dla bezpieczeństwa.

Przestępstwa przeciwko wiarygodności dokumentów i oszustwa dotyczące tożsamości ułatwiają przemyt migrantów, handel ludźmi, ukryte działania przestępcze i handel nielegalnymi towarami. **Detektor wielokrotnych tożsamości**[23], gdy zostanie uruchomiony, zwiększy zdolność organów krajowych do identyfikowania osób posługujących się wieloma tożsamościami i przeciwdziałania oszustwom dotyczącym tożsamości. Komisja zbada sposoby zwiększenia bezpieczeństwa dokumentów podróży i dokumentów pobytowych wydawanych obywatelom UE i obywatelom państw trzecich. Ponadto Komisja oceni, w jaki sposób europejskie portfele tożsamości cyfrowej, które mają zostać wprowadzone na podstawie europejskich ram tożsamości cyfrowej do końca 2026 r., mogą przyczynić się do zwiększenia bezpieczeństwa dokumentów podróży i poprawy weryfikacji tożsamości. Będzie to uzupełnieniem wniosków dotyczących cyfrowych poświadczeń podróżnych i aplikacji EU Digital Travel[24].

Informacje o podróży mają kluczowe znaczenie dla organów, aby mogły identyfikować przemieszczanie się przestępców, terrorystów i innych osób stwarzających zagrożenie bezpieczeństwa i prowadzić dochodzenia w ich sprawie. Chociaż istnieją unijne ramy dotyczące informacji o komercyjnych podróżach lotniczych[25], przetwarzanie danych z innych rodzajów transportu do celów egzekwowania prawa jest fragmentaryczne. W związku z tym

[22] W szczególności system wjazdu/wyjazdu (EES) umożliwi państwom członkowskim identyfikację obywateli państw trzecich na granicach zewnętrznych strefy Schengen oraz rejestrowanie ich wjazdów i wyjazdów, co umożliwi systematyczną identyfikację osób przekraczających okres dozwolonego pobytu. Przed przybyciem obywatela państwa trzeciego na granice zewnętrzne europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) oraz wizowy system informacyjny (VIS) umożliwią państwom członkowskim wstępną ocenę, czy obecność obywatela państwa trzeciego na terytorium UE stanowiłaby zagrożenie dla bezpieczeństwa.

[23] Detektor wielokrotnych tożsamości jest jednym z elementów interoperacyjności wprowadzonych rozporządzeniem (UE) 2019/818 i rozporządzeniem 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/pl/ip_24_5047.

[25] Ramy dotyczące danych dotyczących przelotu pasażera (PNR) i danych pasażera przekazywanych przed podróżą (API) ustanowione dyrektywą (UE) 2016/681 („dyrektywa w sprawie PNR") oraz rozporządzeniem (UE) 2025/12 i rozporządzeniem (UE) 2025/13 („rozporządzenia w sprawie API").

przestępcy i terroryści mogą wykorzystywać różne rodzaje transportu do nielegalnej działalności, która pozostaje niewykryta. Komisja będzie współpracować z państwami członkowskimi i branżą transportową w celu **wzmocnienia ram informacji o podróży** poprzez zbadanie unijnego systemu zobowiązującego operatorów lotów prywatnych do gromadzenia i przekazywania danych pasażerów, ocenę przepisów dotyczących przetwarzania danych dotyczących przelotu pasażera oraz ocenę sposobów usprawnienia przetwarzania informacji o podróżach morskich. W odniesieniu do transportu drogowego Komisja oceni szersze wykorzystanie systemów **automatycznego rozpoznawania tablic rejestracyjnych (ARTR)** i zwiększy możliwości synergii z SIS.

Podejście oparte na prognozowaniu, innowacjach i zdolnościach

Komisja opracuje **kompleksowe podejście prognostyczne w zakresie bezpieczeństwa wewnętrznego na szczeblu UE**, opierając się na najlepszych praktykach określonych na szczeblu krajowym. Podejście to będzie wspierać kształtowanie polityki i wytyczać kierunki inwestycji w odpowiednie badania naukowe i innowacje w dziedzinie bezpieczeństwa finansowane przez UE.

Badania naukowe i innowacje odgrywają kluczową rolę w bezpieczeństwie wewnętrznym poprzez tworzenie rozwiązań służących przeciwdziałaniu pojawiającym się zagrożeniom, w tym wynikającym z niewłaściwego wykorzystania technologii[26]. UE musi nadal inwestować, za pośrednictwem finansowanych przez UE badań naukowych i innowacji w dziedzinie bezpieczeństwa[27], w opracowywanie innowacyjnych narzędzi i rozwiązań służących przeciwdziałaniu zagrożeniom bezpieczeństwa, przy jednoczesnym przestrzeganiu przepisów UE i praw podstawowych. Komisja powinna wspierać przejście od etapu badań naukowych do etapu wdrożenia, aby zapewnić skuteczne wykorzystanie tych nowoczesnych zdolności, traktując priorytetowo **nowoczesne technologie**, takie jak sztuczna inteligencja. Podejście to powinno obejmować szkolenia mające na celu poprawę wykorzystania systemów sztucznej inteligencji i innych zdolności technicznych przez organy ścigania i organy sądowe. Ponadto, w stosownych przypadkach, potencjał technologii podwójnego zastosowania powinien być wykorzystywany w obu kierunkach (wykorzystywanie technologii z sektora cywilnego w sektorze obronnym i z sektora obronnego w sektorze cywilnym)[28].

Unijne centrum innowacji na rzecz bezpieczeństwa wewnętrznego[29] – sieć laboratoriów innowacji zapewniających najnowsze informacje na temat innowacji oraz skuteczne rozwiązania wspierające pracę podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne w UE i państwach członkowskich – pomoże zintegrować badania naukowe z praktyką i polityką. Zwiększenie skuteczności Europolu wymaga rozbudowy repozytorium narzędzi Europolu (ETR), które umożliwiłoby mu identyfikację, opracowywanie, wspólne zamawianie i stosowanie zaawansowanych technologii do działań operacyjnych. Ponadto Komisja utworzy we Wspólnym Centrum Badawczym skupiający naukowców **kampus badań naukowych i innowacji w dziedzinie bezpieczeństwa**, który będzie miał za zadanie skrócić cykl od

[26] Zob. sprawozdanie Wspólnego Centrum Badawczego Komisji pt. „Emerging risks and opportunities for EU internal security stemming from new technologies" [Pojawiające się zagrożenia i możliwości dla bezpieczeństwa wewnętrznego UE wynikające z nowych technologii] https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025 [Badanie na temat wzmocnienia finansowanych przez UE badań naukowych i innowacji w dziedzinie bezpieczeństwa – 20 lat finansowanych przez UE badań naukowych i innowacji w dziedzinie bezpieczeństwa cywilnego – 2025 r.], https://data.europa.eu/doi/10.2837/0004501.

[28] Jak określono w sprawozdaniu Sauliego Niinistö.

[29] Unijne centrum innowacji na rzecz bezpieczeństwa wewnętrznego | Europol.

wyników badań naukowych do innowacji, rozwoju i pomyślnego wdrożenia, przy jednoczesnym obniżeniu kosztów rozwoju, testowania i walidacji.

Nasza **europejska przestrzeń badawcza** ze względu na swój charakter opiera się na współpracy, a zatem jest podatna na obcą ingerencję i dezinformację. Po przyjęciu zalecenia Rady w sprawie bezpieczeństwa badań naukowych[30] Komisja i państwa członkowskie podejmują działania mające na celu wzmocnienie pozycji odpowiednich podmiotów, między innymi poprzez utworzenie europejskiego ośrodka wiedzy fachowej w zakresie bezpieczeństwa badań naukowych.

Kluczowe działania

Komisja przyjmie:

- **wniosek ustawodawczy mający na celu przekształcenie Europolu w prawdziwie operacyjny organ ścigania w 2026 r.;**
- **wniosek ustawodawczy mający na celu wzmocnienie uprawnień Eurojustu w 2026 r.;**
- **wniosek ustawodawczy mający na celu wzmocnienie roli i zwiększenie zakresu zadań Fronteksu w 2026 r.;**
- **wniosek ustawodawczy w sprawie ustanowienia europejskiego systemu łączności krytycznej w 2026 r.**

Komisja:

- **przedstawi w 2025 r. plan działania określający dalsze kroki w zakresie zgodnego z prawem i skutecznego dostępu do danych na potrzeby egzekwowania prawa;**
- **przygotuje w 2025 r. ocenę skutków w celu aktualizacji przepisów dotyczących zatrzymywania danych na szczeblu UE, w stosownych przypadkach;**
- **przedstawi w 2026 r. plan działania w zakresie technologii dotyczący szyfrowania, aby określić i ocenić rozwiązania technologiczne umożliwiające organom ścigania zgodny z prawem dostęp do danych;**
- **będzie pracować nad utworzeniem grupy wysokiego szczebla w celu usprawnienia współpracy operacyjnej w zakresie egzekwowania prawa;**
- **utworzy w 2026 r. kampus badań naukowych i innowacji w dziedzinie bezpieczeństwa we Wspólnym Centrum Badawczym.**

Komisja, we współpracy z państwami członkowskimi i odpowiednimi agencjami UE:

- **wzmocni architekturę EMPACT;**
- **będzie dążyć do szybkiego wprowadzenia architektury interoperacyjności i wdrożenia rozporządzenia Prüm II;**
- **wzmocni ramy informacji o podróży.**

Państwa członkowskie wzywa się do:

- **transpozycji i pełnego wdrożenia dyrektywy w sprawie wymiany informacji.**

[30] Dz.U. C, C/2024/3510, 30.5.2024.

4. Odporność na zagrożenia hybrydowe i inne wrogie działania

Będziemy budować odporność na zagrożenia hybrydowe poprzez zwiększenie ochrony infrastruktury krytycznej, wzmocnienie cyberbezpieczeństwa, zabezpieczenie węzłów transportowych i portów oraz zwalczanie zagrożeń w internecie.

Częstotliwość i wyrafinowanie wrogich działań podważających bezpieczeństwo UE wzrosły, a podmioty działające w złym zamiarze znacznie rozszerzyły swój arsenał. Nasiliły się kampanie hybrydowe wymierzone w UE, jej państwa członkowskie i partnerów, obejmujące akty sabotażu skierowane przeciwko infrastrukturze krytycznej, podpalenia, cyberataki, ingerencje w wybory, zagraniczne manipulacje informacjami i ingerencje w informacje, w tym dezinformację, oraz wykorzystywanie migracji jako broni. Instytucje, organy i jednostki organizacyjne Unii („podmioty unijne"), ze względu na swoją rolę polityczną i operacyjną oraz charakter przetwarzanych przez nie informacji, również stały się celem wrogich działań.

UE musi **zwiększyć swoją odporność**, skutecznie wykorzystywać obecne narzędzia i opracować nowe sposoby radzenia sobie ze zmieniającymi się zagrożeniami ze strony podmiotów państwowych i niepaństwowych, zarówno teraz, jak i w przyszłości.

Infrastruktura krytyczna

Zagrożenia dla **infrastruktury krytycznej**, w tym zagrożenia hybrydowe, takie jak sabotaż i szkodliwe działanie w cyberprzestrzeni, stanowią poważny problem, zwłaszcza w odniesieniu do infrastruktury łączącej państwa członkowskie, np. rurociągów międzysystemowych lub transgranicznych kabli komunikacyjnych, oraz transportu. Od czasu wojny napastniczej Rosji przeciwko Ukrainie akty sabotażu wymierzone w infrastrukturę krytyczną nasiliły się, zwłaszcza w 2024 r., dotykając wiele państw członkowskich. Współpraca między organami ścigania, służbami bezpieczeństwa i cyberbezpieczeństwa, wojskiem i służbami ochrony ludności oraz podmiotami prywatnymi ma zasadnicze znaczenie dla skutecznego przewidywania takich działań, ich wykrywania, zapobiegania im i reagowania na nie.

Zmniejszenie podatności na zagrożenia i wzmocnienie odporności podmiotów krytycznych jest niezbędne, aby zapewnić nieprzerwane świadczenie usług kluczowych o podstawowym znaczeniu dla gospodarki i społeczeństwa. W związku z tym kluczowe znaczenie w tym względzie ma terminowa transpozycja i prawidłowe wdrożenie przez wszystkie państwa członkowskie **dyrektywy w sprawie odporności podmiotów krytycznych (dyrektywa CER)**[31] oraz **dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2)**[32].

Aby zapewnić szybkie postępy, Komisja będzie wspierać państwa członkowskie w identyfikowaniu podmiotów krytycznych[33] i wymianie dobrych praktyk w zakresie strategii krajowych i ocen ryzyka w odniesieniu do usług kluczowych, we współpracy z **Grupą ds. Odporności Podmiotów Krytycznych i grupą współpracy NIS**. W przypadku wystąpienia zakłóceń w funkcjonowaniu infrastruktury krytycznej o znaczącym wpływie transgranicznym do celów koordynacji odpowiedzi na szczeblu UE służyć będzie **plan działania dotyczący skoordynowanej reakcji na zakłócenia infrastruktury krytycznej o istotnym znaczeniu**

[31] 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.

[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

[33] Do sektorów objętych dyrektywą należą: energetyka, transport, bankowość, infrastruktura rynku finansowego, zdrowie, woda pitna, ścieki, infrastruktura cyfrowa, administracja publiczna, przestrzeń kosmiczna oraz produkcja, przetwarzanie i dystrybucja żywności.

transgranicznym. Komisja zachęca Radę do szybkiego przyjęcia **unijnego planu działania na rzecz cyberbezpieczeństwa**, który jeszcze bardziej poprawi koordynację w kontekście zarządzania kryzysowego, ułatwiając ściślejszą współpracę między organami w zakresie odporności fizycznej i cyfrowej. Po udanych testach warunków skrajnych w sektorze energetycznym w 2023 r. Komisja będzie promować **dobrowolne testy warunków skrajnych** w innych sektorach kluczowych dla bezpieczeństwa wewnętrznego. Ponadto Komisja przedstawi **ogólnounijny przegląd transgranicznych i międzysektorowych czynników ryzyka** dla usług kluczowych, aby wesprzeć oceny ryzyka przeprowadzane przez państwa członkowskie i poinformować o kompleksowej ocenie ryzyka na szczeblu UE. Zgodnie ze strategią na rzecz unii gotowości Komisja będzie współpracować z państwami członkowskimi w celu określenia kolejnych sektorów i usług nieobjętych obecnymi przepisami, w odniesieniu do których może zaistnieć potrzeba podjęcia działań.

Grupa Zadaniowa UE–NATO ds. Odporności Infrastruktury Krytycznej przyczyniła się do doskonałej współpracy w zakresie wymiany najlepszych praktyk i zwiększania odporności w sektorach energii, transportu, infrastruktury cyfrowej oraz sektorze kosmicznym. Prace te będą kontynuowane w ramach **zorganizowanego dialogu UE–NATO na temat odporności**. **Unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym** oferuje państwom członkowskim i partnerom solidne wsparcie w przygotowaniu się na zagrożenia hybrydowe i przeciwdziałaniu im. **Unijne zespoły szybkiego reagowania na zagrożenia hybrydowe**[34] zapewniają państwom członkowskim, różnym misjom i partnerom UE, na ich wniosek, pomoc krótkoterminową dostosowaną do ich potrzeb. Ponadto Komisja będzie kontynuować współpracę UE w zakresie zwalczania sabotażu poprzez działania eksperckie[35], w tym **specjalny wspólny program prac** dla ekspertów mający na celu usprawnienia wymiany informacji i określenia środków przeciwdziałania.

Incydenty, których celem są **kable podmorskie** w Europie, uwypuklają potrzebę wprowadzenia bardziej zdecydowanych środków i jaśniejszych reakcji. Jak określono w **planie działania UE na rzecz bezpieczeństwa kabli**[36], Komisja, wraz z wysoką przedstawicielką, będzie współpracować z państwami członkowskimi, agencjami UE i partnerami, takimi jak NATO, w celu zapobiegania zagrożeniom dla kabli podmorskich, ich wykrywania, reagowania na nie i zapobiegania im. Aby opracować zintegrowany obraz sytuacji w dziedzinie zagrożeń, Komisja będzie współpracować z państwami członkowskimi w celu opracowania i wdrożenia, na zasadzie dobrowolności, zintegrowanego mechanizmu nadzoru nad kablami podmorskimi w każdym basenie morskim, począwszy od regionalnego węzła nordycko-bałtyckiego.

Cyberbezpieczeństwo

Uporczywość **szkodliwych działań w cyberprzestrzeni**, które często stanowią część szerszego zakresu wielowymiarowych i hybrydowych zagrożeń, wymaga ciągłej uwagi i działań na szczeblu europejskim. W ostatnich latach Unia przyjęła szereg przepisów dotyczących cyberbezpieczeństwa, które wzmacniają cyberodporność podmiotów NIS 2 działających w sektorach krytycznych UE, a także podmiotów unijnych[37], poprawiają bezpieczeństwo produktów cyfrowych (akt dotyczący cyberodporności) oraz ustanawiają ramy

[34] Strategiczny kompas UE na rzecz bezpieczeństwa i obrony z 2022 r., s. 22.
[35] Doradcy UE ds. zapewniania bezpieczeństwa, europejska sieć niszczenia amunicji wybuchowej (EEODN), sieć Atlas, unijna sieć ds. bezpieczeństwa w miejscach wysokiego ryzyka (EU HRSN), grupa doradcza ds. bezpieczeństwa CBRJ, Grupa ds. Odporności Podmiotów Krytycznych (CERG).
[36] JOIN(2025) 9 final.
[37] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii, Dz.U. L, 2023/2841, 18.12.2023.

gotowości i wsparcia w zakresie reagowania na incydenty (akt w sprawie cybersolidarności). W styczniu 2025 r. Komisja przyjęła **europejski plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców**[38] w celu poprawy wykrywania zagrożeń, gotowości i reagowania kryzysowego. Jego pełne wdrożenie jest kluczowe. Jednocześnie, aby stawić czoła nowym zagrożeniom i zmianom, musimy zintensyfikować nasze działania, w szczególności w dziedzinie wymiany informacji, bezpieczeństwa łańcucha dostaw, oprogramowania szantażującego i cyberataków, a także suwerenności technologicznej.

Ponadto wdrożenia wymaga likwidacja niedoboru wykwalifikowanej siły roboczej w dziedzinie cyberbezpieczeństwa wynoszącego 299 000 osób. Komisja będzie współpracować z państwami członkowskimi w ramach unii umiejętności[39], aby powiększyć liczbę osób zatrudnionych w dziedzinie cyberbezpieczeństwa, w szczególności poprzez wykorzystanie nowej Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Strategiczny plan w dziedzinie kształcenia STEM[40] przyczynia się do zwiększenia rezerwy talentów i reagowania Europy na potrzeby rynku pracy w dziedzinie cyberbezpieczeństwa.

Równolegle do zwiększania swojej odporności UE będzie nadal w pełni wykorzystywać ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni (**zestaw narzędzi dla dyplomacji cyfrowej**), aby zapobiegać zagrożeniom cyberbezpieczeństwa ze strony podmiotów państwowych i niepaństwowych, powstrzymywać je i reagować na nie.

Bezpieczeństwo łańcuchów dostaw ICT

Unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G zapewnia odpowiednie ramy ochrony sieci 5G, ale obecnie nie jest w wystarczającym stopniu wdrażany przez państwa członkowskie. Nadal istnieją niedopuszczalne zagrożenia dla bezpieczeństwa, w szczególności jeśli chodzi o zastępowanie dostawców wysokiego ryzyka. Zharmonizowane podejście do bezpieczeństwa łańcucha dostaw ICT może zaradzić obecnej fragmentacji rynku wewnętrznego spowodowanej różnymi podejściami na szczeblu krajowym, pozwoli uniknąć krytycznych zależności i zmniejszyć ryzyko naszych łańcuchów dostaw ICT od dostawców wysokiego ryzyka, zabezpieczając w ten sposób naszą infrastrukturę krytyczną.

Zgodnie z tym podejściem, w ramach zbliżającego się **przeglądu aktu o cyberbezpieczeństwie**, Komisja przeanalizuje w szerszym zakresie bezpieczeństwo i odporność łańcuchów dostaw ICT i infrastruktury ICT. Ponadto Komisja zaproponuje udoskonalenie **europejskich ram certyfikacji cyberbezpieczeństwa**, aby zapewnić terminowe przyjmowanie przyszłych systemów certyfikacji i reagowanie na potrzeby polityczne.

W oparciu o istniejące lub trwające oceny sektorowe[41] Komisja wraz z państwami członkowskimi opracuje **strategiczne planowanie skoordynowanych ocen ryzyka w cyberprzestrzeni.**

Usługi w chmurze i usługi telekomunikacyjne stały się podstawowym elementem łańcuchów dostaw infrastruktury krytycznej, przedsiębiorstw i organów publicznych. Komisja podejmie działania, aby zachęcić podmioty krytyczne do wyboru **usług w chmurze i usług telekomunikacyjnych, które oferują odpowiedni poziom cyberbezpieczeństwa**,

[38] https://digital-strategy.ec.europa.eu/pl/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Takie jak dotyczące sieci 5G, telekomunikacji, energii elektrycznej, energii ze źródeł odnawialnych i pojazdów podłączonych do sieci.

z uwzględnieniem nie tylko ryzyka technicznego, ale również ryzyka strategicznego i zależności.

Oprogramowanie szantażujące i cyberataki

Stałym poważnym wyzwaniem w UE i na świecie jest **oprogramowanie szantażujące**, a w jednym ze sprawozdań szacuje się, że do 2031 r. globalne roczne koszty z nim związane wyniosą ponad 250 mld EUR[42]. Zarówno **dyrektywa NIS 2**, jak i **akt dotyczący cyberodporności** znacznie poprawią stan bezpieczeństwa podmiotów, sprawiając, że przeprowadzanie ataków przez siatki posługujące się oprogramowaniem szantażującym będzie bardziej kosztowne. Ponadto Komisja będzie ściśle współpracować z państwami członkowskimi w celu zapewnienia, aby więcej ataków z użyciem oprogramowania szantażującego, w szczególności zaawansowanych utrzymujących się zagrożeń, oraz płatności okupu było zgłaszanych organom ścigania, co ułatwi prowadzenie dochodzeń.

Aby zapobiegać cyberatakom i je powstrzymywać, UE musi zintensyfikować wymianę informacji między organami ścigania, organami i podmiotami ds. cyberbezpieczeństwa, a także podmiotami prywatnymi, pod egidą Europolu i Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

Europol i Eurojust powinny nadal bazować na swoich osiągnięciach w zakresie likwidacji operacji związanych z oprogramowaniem szantażującym i wspierać współpracę organów ścigania. W tym celu organy ścigania powinny zmaksymalizować wykorzystanie mechanizmów współpracy, m.in. **opracowanego przez Europol międzynarodowego modelu reagowania na oprogramowanie szantażujące** oraz **międzynarodowej inicjatywy na rzecz walki z oprogramowaniem szantażującym**[43], a ENISA i Europol powinny współpracować w celu rozszerzenia repozytorium narzędzi deszyfrujących dla różnych odmian oprogramowania szantażującego[44].

Suwerenność technologiczna

Cyberbezpieczeństwo i suwerenność technologiczna są ze sobą ściśle powiązane, a zależnościami technologicznymi należy zająć się w pierwszej kolejności. Unia musi **kierować rozwojem i wdrażaniem nowych technologii**, a Komisja powinna pracować nad **zwiększeniem zdolności w zakresie technologii strategicznych**, takich jak sztuczna inteligencja, komputery kwantowe, zaawansowana łączność, chmura obliczeniowa, technologie przetwarzania brzegowego i internet rzeczy[45], za pośrednictwem przyszłych inicjatyw, takich jak plan działania na rzecz kontynentu sztucznej inteligencji, strategia kwantowa i inne[46]. Komisja będzie nadal wspierać terminowe wdrażanie najnowszych dostępnych **protokołów internetowych** uzgodnionych na szczeblu międzynarodowym, które mają zasadnicze znaczenie dla utrzymania skalowalnego i wydajnego internetu o podwyższonym poziomie cyberbezpieczeństwa. Konieczne są również dalsze działania w celu sprostania **wyzwaniom związanym z widmem radiowym**, takim jak spoofing GNSS, zagłuszanie, ryzyko związane z łańcuchem dostaw i zależności, takie jak wykorzystanie

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Dostępne za pośrednictwem projektu No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_pl#step-scope.
[46] Np. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, inicjatywa przewodnia w dziedzinie technologii kwantowych strona główna Quantum Flagship | Quantum Flagship, sieci 3C (COM(2024) 81 final) i plan działania UE na rzecz bezpieczeństwa kabli (JOIN(2025) 9 final).

technologii wykrywania kwantowego i badanie rozwoju zdolności monitorowania częstotliwości radiowych.

Wdrożenie rozwiązań w zakresie **kryptografii postkwantowej** będzie miało kluczowe znaczenie dla zabezpieczania komunikacji szczególnie chronionej, przechowywanych danych oraz dla ochrony tożsamości cyfrowych w nowej erze kwantowej. Na podstawie zalecenia z 2024 r. w sprawie skoordynowanego planu wdrożenia dotyczącego przejścia na kryptografię postkwantową[47] Komisja prowadzi współpracę z państwami członkowskimi w celu wspierania tego przejścia. W związku z tym państwa członkowskie powinny jak najszybciej i nie później niż do końca 2030 r. zidentyfikować przypadki wysokiego ryzyka w podmiotach krytycznych i zapewnić szyfrowanie odporne na technologie kwantowe w odniesieniu do tych przypadków wysokiego ryzyka. Komisja współpracuje również z państwami członkowskimi i Europejską Agencją Kosmiczną (ESA) w celu opracowania i wdrożenia **europejskiej infrastruktury komunikacji kwantowej (EuroQCI)**[48] w oparciu o kwantową dystrybucję klucza (QKD) w ramach **IRIS²**, unijnego programu bezpiecznej łączności. Obie inicjatywy ostatecznie umożliwią podmiotom bezpieczne przesyłanie danych i przechowywanie informacji.

Technologie kwantowe będą również odgrywać kluczową rolę w zastosowaniach związanych z bezpieczeństwem: w ramach **strategii kwantowej** opracowany zostanie **plan działania dotyczący wykrywania kwantowego w zastosowaniach związanych z bezpieczeństwem**. W tym samym duchu Komisja pracuje nad uodparnianiem swoich korporacyjnych systemów o kluczowym znaczeniu dla bezpieczeństwa, w tym swoich niejawnych systemów informatycznych, na technologie kwantowe.

Ramy cyberbezpieczeństwa przyjazne dla biznesu

Zbliżający się przegląd aktu o cyberbezpieczeństwie jest okazją do **uproszczenia unijnych przepisów dotyczących cyberbezpieczeństwa**, zgodnie z Kompasem konkurencyjności dla UE. Komisja będzie ściśle współpracować z państwami członkowskimi w celu zapewnienia szybkiego, spójnego i przyjaznego dla biznesu wdrożenia horyzontalnych ram cyberbezpieczeństwa określonych w dyrektywie NIS 2, akcie dotyczącym cyberodporności i akcie w sprawie cybersolidarności, promując prostotę i spójność oraz unikając fragmentacji lub powielania przepisów dotyczących cyberbezpieczeństwa w przepisach unijnych i krajowych.

Aby umożliwić bezpieczny dostęp do usług online i wzmocnić bezpieczeństwo cyfrowe w całej UE, poprzez **europejskie ramy tożsamości cyfrowej** zaoferowane zostaną wszystkim obywatelom i mieszkańcom UE godne zaufania portfele tożsamości cyfrowej przed końcem 2026 r. Przyszły **europejski portfel biznesowy** ułatwi bezpieczne transgraniczne interakcje między przedsiębiorstwami a administracją publiczną. Oba te elementy są warunkiem wstępnym bezpiecznego i skuteczniejszego funkcjonowania jednolitego rynku opartego na danych, z narzędziami takimi jak jednolity portal cyfrowy, fakturowanie elektroniczne, e-zamówienia i cyfrowy paszport produktu.

Bezpieczeństwo w internecie

Niektóre z najpoważniejszych zagrożeń hybrydowych zagrażających bezpieczeństwu ludzi w Europie i wymierzonych w sferę demokratyczną UE mają miejsce w internecie. Zagrożenia te obejmują nielegalną działalność i nielegalne treści w internecie, manipulacje informacją

[47] Zalecenie w sprawie skoordynowanego planu wdrożenia dotyczącego przejścia na kryptografię postkwantową | Kształtowanie cyfrowej przyszłości Europy.
[48] https://digital-strategy.ec.europa.eu/pl/policies/european-quantum-communication-infrastructure-euroqci.

polegające na sztucznym nagłaśnianiu, informacje wprowadzające w błąd oraz zagraniczne manipulacje informacjami i ingerencje w informacje.

Rygorystyczne egzekwowanie przepisów **aktu o usługach cyfrowych** ma zasadnicze znaczenie dla zapewnienia bezpiecznego i dostępnego środowiska internetowego z podmiotami ponoszącymi odpowiedzialność, odpornego również na zagrożenia hybrydowe. W akcie o usługach cyfrowych zobowiązuje się dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych do przeprowadzania ocen ryzyka i wprowadzania środków ograniczających ryzyko systemowe wynikające z projektowania i funkcjonowania ich usług lub korzystania z nich. Ryzyko takie może obejmować negatywny wpływ na dyskurs obywatelski i procesy wyborcze, a także na bezpieczeństwo publiczne, taki jak daleko idąca ingerencja zagranicznych podmiotów państwowych działających w złej wierze, na przykład w procesy wyborcze. Ważne jest szkolenie właściwych organów państw członkowskich w zakresie stosowania narzędzi prawnych do szybkiego usuwania nielegalnych treści w internecie, w szczególności w odniesieniu do cyberprzemocy ze względu na płeć. W akcie o usługach cyfrowych przewidziano mechanizm reagowania kryzysowego, który można uruchomić w przypadku wystąpienia nadzwyczajnych okoliczności prowadzących do poważnego zagrożenia bezpieczeństwa publicznego lub zdrowia publicznego w Unii lub na znacznych jej obszarach. Aby uzupełnić ten mechanizm, Komisja i właściwe organy krajowe wyznaczone na koordynatorów ds. usług cyfrowych opracowały również dobrowolne **ramy reagowania na incydenty związane z aktem o usługach cyfrowych**. Koordynatorzy ds. usług cyfrowych podjęli również działania mające pomóc w ochronie uczciwości wyborów, na przykład organizując obrady okrągłego stołu poświęcone wyborom i testy warunków skrajnych[49]. Akt o usługach cyfrowych, wraz z rozporządzeniem w sprawie reklamy politycznej[50], stanowi jeden z kilku elementów związanych z ochroną demokracji i integralności procesów demokratycznych, które są narażone na ataki wrogich podmiotów, w tym za pomocą narzędzi cyfrowych i mediów społecznościowych.

Kolejnym ważnym elementem oferującym kluczowe wsparcie na szczeblu UE jest wdrożenie zestawu narzędzi **przeciwdziałania zagranicznymi manipulacjami informacjami i ingerencjami w informacje**. Kluczowe znaczenie dla tych wysiłków ma również wspieranie umiejętności cyfrowych i umiejętności korzystania z mediów oraz krytycznego myślenia[51].

Przeciwdziałanie wykorzystywaniu migracji jako broni

Rosja, z pomocą Białorusi i przy jej zdecydowanym wsparciu, celowo wykorzystuje migrację jako broń i nielegalnie ułatwia przepływy migracyjne w kierunku granic zewnętrznych UE w celu destabilizacji unijnych społeczeństw i podważenia jedności Unii Europejskiej. Zagraża to nie tylko bezpieczeństwu narodowemu i suwerenności państw członkowskich, lecz również bezpieczeństwu i integralności strefy Schengen oraz bezpieczeństwu całej Unii. W swoich konkluzjach z października 2024 r. Rada Europejska podkreśliła, że nie wolno pozwalać Rosji i Białorusi ani żadnemu innemu państwu na nadużywanie unijnych wartości, w tym prawa do azylu, ani na osłabianie unijnej demokracji.

Jak stwierdzono w komunikacie Komisji z 2024 r. w sprawie wykorzystywania migracji jako broni, oprócz udzielenia silnego wsparcia politycznego Unia podjęła działania finansowe, operacyjne i dyplomatyczne, w tym współpracę z krajami pochodzenia i tranzytu, w celu

[49] Podręcznik na temat wyborów dla koordynatorów ds. usług cyfrowych z 2025 r. związany z aktem o usługach cyfrowych https://digital-strategy.ec.europa.eu/pl/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/900 z dnia 13 marca 2024 r. w sprawie przejrzystości i targetowania reklamy politycznej, Dz.U. L, 2024/900, 20.3.2024.

[51] Plan działania w dziedzinie edukacji cyfrowej (2021–2027) – europejski obszar edukacji.

skutecznego przeciwdziałania tym zagrożeniom[52]. Reakcja ta polega na wykorzystaniu nowych ram ustanowionych przez Radę do nakładania sankcji na osoby i organizacje zaangażowane w działania i polityki, takie jak wykorzystywanie przez Rosję migracji jako broni, poprzez zamrożenie aktywów i zakaz podróżowania[53]. W razie potrzeby UE będzie nadal korzystać z tych ram i wspierać państwa członkowskie w przeciwdziałaniu temu zagrożeniu.

Bezpieczeństwo transportu

Porty morskie, porty lotnicze i infrastruktura lądowa to kluczowe punkty wejścia i wyjścia. Odgrywają one kluczową rolę w gospodarce i społeczeństwie UE oraz mają zasadnicze znaczenie dla mobilności wojskowej. Jednak te węzły transportowe i środki transportu są również głównymi celami zagrożeń zewnętrznych i działalności przestępczej. Niedawne incydenty, w tym naruszenia ochrony ładunków lotniczych i ataki na infrastrukturę kolejową, uwidaczniają poważne zagrożenia. **Przewoźnicy** mogą być zarówno celem, jak i narzędziem dla podmiotów działających w złym zamiarze. Istniejące instrumenty prawne UE zwiększyły ochronę lotnictwa[54], jednak wysoki poziom zagrożenia dla lotnictwa cywilnego wymaga środków przewidywania incydentów i szybkich konsultacji z odpowiednimi państwami członkowskimi. Komisja będzie współpracować z państwami członkowskimi w celu zmiany obowiązujących przepisów wykonawczych w dziedzinie ochrony lotnictwa na potrzeby wymiany informacji niejawnych dotyczących **zdarzeń związanych z ochroną lotnictwa**. Ponadto Komisja rozważy **środki regulacyjne** mające na celu przeciwdziałanie nowym zagrożeniom, takim jak **incydenty związane z ładunkami lotniczymi**, oraz wzmocnienie norm ochrony lotnictwa. Obejmie to również udoskonalenia **przepisów w zakresie ochrony lotnictwa**, aby umożliwić wprowadzenie natychmiastowych środków reagowania, przy jednoczesnym utrzymaniu jednolitego obszaru ochrony w portach lotniczych UE.

Opracowując przyszłą **strategię UE w sprawie portów**, w oparciu o **sojusz portów europejskich**, Komisja zbada sposoby dalszego udoskonalenia przepisów dotyczących bezpieczeństwa morskiego, aby skutecznie reagować na pojawiające się zagrożenia, zabezpieczyć porty i zwiększyć bezpieczeństwo łańcucha dostaw UE. W tym celu Komisja zapewni jej skuteczne wdrożenie oraz będzie pracować nad harmonizacją praktyk krajowych i zaostrzeniem sprawdzania przeszłości w portach. W nawiązaniu do protokołów bezpieczeństwa ustanowionych dla ładunków lotniczych Komisja będzie współpracować z państwami członkowskimi i sektorem prywatnym nad rozszerzeniem tych protokołów w celu zabezpieczenia łańcuchów transportu morskiego.

Proponowany Urząd UE ds. Celnych przeanalizuje i oceni ryzyko w oparciu o **informacje celne** dotyczące towarów wprowadzanych do UE, wywożonych z UE i przewożonych przez jej terytorium, aby wspierać państwa członkowskie w zapobieganiu wykorzystywaniu międzynarodowych łańcuchów dostaw przez podmioty działające w złym zamiarze. Zgodnie ze strategią Unii Europejskiej w zakresie bezpieczeństwa morskiego[55] przyszły **europejski pakt na rzecz oceanów** odegra kluczową rolę w zwiększaniu bezpieczeństwa morskiego w basenach morskich wokół UE i poza nią, w tym poprzez zachęcanie do zwiększenia skali wielozadaniowych operacji i ćwiczeń na morzu.

Odporność łańcuchów dostaw

[52] COM(2024) 570 final.
[53] Rozporządzenie Rady (UE) 2024/2642 z dnia 8 października 2024 r. dotyczące środków ograniczających w związku z działaniami destabilizującymi Rosji, ST/8744/2024/INIT, Dz.U. L, 2024/2642, 9.10.2024.
[54] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego, Dz.U. L 97 z 9.4.2008, s. 72.
[55] JOIN(2023) 8 final.

Europa musi w mniejszym stopniu polegać na technologii państw trzecich, w przeciwnym razie obecna sytuacja może prowadzić do uzależnienia i zagrożeń dla bezpieczeństwa. Komisja dąży do ograniczenia zależności od jednego dostawcy zagranicznego, zmniejszenia ryzyka w łańcuchach dostaw od dostawców wysokiego ryzyka oraz zabezpieczenia infrastruktury krytycznej i zdolności przemysłowych na terytorium UE, jak określono w **Kompasie konkurencyjności dla UE**[56] i w **Pakcie dla czystego przemysłu**[57]. Komisja będzie promować **politykę przemysłową na rzecz bezpieczeństwa wewnętrznego** poprzez współpracę z przemysłem UE w kluczowych sektorach (jak np. węzły transportowe, infrastruktura krytyczna) w celu opracowania rozwiązań w zakresie bezpieczeństwa, takich jak urządzenia do wykrywania, technologie biometryczne i bezzałogowe statki powietrzne, z uwzględnieniem zabezpieczeń już na etapie projektowania. Dokonując **przeglądu unijnych przepisów dotyczących zamówień publicznych**, Komisja oceni, czy względy bezpieczeństwa zawarte w dyrektywie w sprawie zamówień w dziedzinach obronności i bezpieczeństwa[58] z 2009 r. są wystarczające, aby zaspokoić potrzeby w zakresie egzekwowania prawa i odporności podmiotów krytycznych.

Komisja będzie wspierać państwa członkowskie w **monitorowaniu bezpośrednich inwestycji zagranicznych (BIZ)** i zamówień na sprzęt dla centrów logistycznych, zapewniając bezpieczeństwo infrastruktury krytycznej i technologii krytycznych.

Akt o sytuacji nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego (IMERA), gdy wejdzie w życie, pomoże UE w zarządzaniu kryzysami zakłócającymi krytyczne łańcuchy dostaw oraz swobodny przepływ towarów, usług i osób. Umożliwi on szybką koordynację kryzysową, identyfikację towarów i usług istotnych w kontekście kryzysu oraz zapewni zestaw narzędzi zapewniających ich dostępność. Ponadto, w ścisłej współpracy z państwami członkowskimi, Komisja zaproponuje ustanowienie **wielopodmiotowego mechanizmu ostrzegania w zakresie bezpieczeństwa transportu i łańcucha dostaw**, aby zagwarantować bezpieczną i terminową wymianę istotnych informacji niezbędnych do przewidywania zagrożeń i przeciwdziałania im.

Ponadto, wraz z wdrożeniem aktu w sprawie surowców krytycznych i aktu w sprawie przemysłu neutralnego emisyjnie, szersze stosowanie kryteriów zrównoważonego rozwoju, odporności i europejskich kryteriów preferencji w zamówieniach publicznych UE będzie sprzyjać rozwojowi rynków pionierskich. Wzmocnione więzi handlowe, na przykład poprzez partnerstwa w dziedzinie surowców oraz czyste partnerstwa handlowo-inwestycyjne, pomogą zdywersyfikować łańcuchy dostaw.

Odporność i gotowość na zagrożenia chemiczne, biologiczne, radiologiczne i jądrowe

Rosyjska wojna napastnicza przeciwko Ukrainie zwiększyła ryzyko **zagrożeń chemicznych, biologicznych, radiologicznych i jądrowych (CBRJ)**. Aby przeciwdziałać potencjalnemu nabywaniu i wykorzystywaniu materiałów CBRJ jako broni, Komisja będzie wspierać państwa członkowskie i kraje partnerskie i zapewniać specjalne szkolenia i ćwiczenia. Komisja zwiększy również gotowość i zdolności reagowania w obszarze CBRJ, określając priorytety w zakresie zagrożeń, finansując innowacje w zakresie środków przeciwdziałania, zdolności rescEU i gromadząc zapasy medycznych środków przeciwdziałania, w ramach nowego **planu działania na rzecz gotowości i reagowania w zakresie CBRJ**. Ponadto **strategia UE**

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Dyrektywa 2009/81/WE w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa, Dz.U. L 216, 20.8.2009.

w zakresie medycznych środków przeciwdziałania będzie wspierać opracowywanie takich środków, począwszy od badań naukowych po produkcję i dystrybucję, aby chronić UE przed pandemiami i zagrożeniami CBRJ.

Opierając się na doświadczeniach związanych z pandemią COVID-19, UE wzmocniła ramy bezpieczeństwa zdrowotnego[59]. Komisja wyznacza laboratoria referencyjne UE w dziedzinie zdrowia publicznego w celu wzmocnienia unijnych i krajowych zdolności w zakresie nadzoru i szybkiego wykrywania. W 2025 r. opublikowany zostanie unijny plan gotowości, zapobiegania i reagowania w zakresie bezpieczeństwa zdrowotnego.

Kluczowe działania

Komisja:

- **dokona w 2025 r. przeglądu i zmiany aktu o cyberbezpieczeństwie;**
- **opracuje środki zapewniające cyberbezpieczeństwo korzystania z usług w chmurze;**
- **zaproponuje w 2025 r. strategię UE w sprawie portów;**
- **dokona w 2026 r. zmiany unijnych przepisów dotyczących zamówień publicznych w dziedzinie obronności i bezpieczeństwa;**
- **przedstawi w 2026 r. nowy plan działania na rzecz gotowości i reagowania w zakresie CBRJ.**

Komisja we współpracy z państwami członkowskimi:

- **opracuje i wdroży europejską infrastrukturę komunikacji kwantowej (EuroQCI);**
- **zapewni skuteczne egzekwowanie przepisów aktu o usługach cyfrowych;**
- **będzie przeciwdziałać wykorzystywaniu migracji jako broni;**
- **ustanowi system zgłaszania zdarzeń związanych z ochroną lotnictwa;**
- **będzie pracować nad ustanowieniem wielopodmiotowego mechanizmu ostrzegania w zakresie bezpieczeństwa transportu i łańcucha dostaw.**

Radę wzywa się do:

- **przyjęcia zalecenia Rady w sprawie unijnego planu działania na rzecz cyberbezpieczeństwa.**

Państwa członkowskie wzywa się do:

- **transpozycji i pełnego wdrożenia dyrektyw CER i NIS 2.**

5. Zaciskanie pętli wokół poważnej i zorganizowanej przestępczości

Pomożemy wyeliminować przestępczość zorganizowaną, proponując surowsze przepisy ukierunkowane na zwalczanie siatek przestępczości zorganizowanej, w tym w zakresie dochodzeń; sprawimy, że młodzież w UE będzie mniej podatna na werbowanie do grup przestępczych, i wzmocnimy środki mające na celu odcięcie dostępu do narzędzi i mienia pochodzącego z działalności przestępczej.

Przestępczość zorganizowana wykorzystuje zmieniającą się sytuację i rozprzestrzenia się w postępie geometrycznym. Korzysta z zaawansowanych technologii, działa w wielu jurysdykcjach i ma silne powiązania poza granicami UE. Biorąc pod uwagę te złożone, transgraniczne zagrożenia, zasadnicze znaczenie ma koordynacja i wsparcie na szczeblu UE.

[59] Przede wszystkim za pomocą rozporządzenia (UE) 2022/2371 w sprawie poważnych transgranicznych zagrożeń zdrowia.

Zapobieganie przestępczości

Werbowanie osób młodych do udziału w przestępczości zorganizowanej jest coraz większym problemem w UE. Zwalczanie przestępczości zorganizowanej wymaga zajęcia się jej **podstawowymi przyczynami** poprzez oferowanie edukacji i alternatywy dla życia przestępczego w ramach podejścia obejmującego całe społeczeństwo. Komisja będzie wspierać włączenie względów bezpieczeństwa do polityki UE w dziedzinie edukacji, polityki społecznej, polityki zatrudnienia i polityki regionalnej. UE będzie **promować opartą na dowodach politykę zapobiegania przestępczości**[60] dostosowaną do warunków lokalnych.

Aby chronić odbiorców usług online, w szczególności małoletnich, przed m.in. niegodziwym traktowaniem dzieci w celach seksualnych, handlarzami ludźmi i werbowaniem w internecie do celów przestępstw lub brutalnego ekstremizmu, środki przewidziane w **akcie o usługach cyfrowych** nakładają na dostawców platform internetowych dostępnych dla małoletnich obowiązek zarządzania ryzykiem i podejmowania działań w przypadku nielegalnych treści, w tym nawoływania do nienawiści. Komisja planuje wydać **wytyczne dotyczące ochrony małoletnich**, aby pomóc dostawcom platform internetowych w zapewnieniu wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich w internecie. Wytyczne będą zawierać zestaw zaleceń dla wszystkich usług cyfrowych prowadzonych w Unii w celu zwiększenia ochrony małoletnich w internecie. W 2025 r. Komisja planuje również ułatwić opracowanie unijnego rozwiązania służącego do **weryfikacji wieku, które będzie chroniło prywatność** i wypełni lukę do czasu zaoferowania portfela europejskiej tożsamości cyfrowej pod koniec 2026 r. Komisja przedstawi również plan działania przeciwko cyberszykanowaniu.

Ponadto Komisja będzie nadal wspierać dobrowolną wielostronną współpracę z platformami internetowymi i innymi odpowiednimi podmiotami, w tym za pośrednictwem Forum UE ds. Internetu i ukierunkowanych kodeksów postępowania na mocy aktu o usługach cyfrowych, takich jak kodeks postępowania dotyczący nielegalnego nawoływania do nienawiści w internecie z 2025 r. Celem jest podnoszenie świadomości, wspólne reagowanie na obecne i pojawiające się zagrożenia oraz opracowywanie i wymiana dobrych praktyk w zakresie środków łagodzących.

Na szczeblu lokalnym wpływ przestępczości zorganizowanej uwypukla potrzebę rozwiązań regionalnych w celu zmniejszenia podatności na zagrożenia i atrakcyjności nielegalnej działalności. Agenda UE dla miast ma zaradzić zagrożeniom bezpieczeństwa w miastach i będzie opierać się na inicjatywie „Miasta UE przeciwko radykalizacji postaw". Komisja będzie wspierać państwa członkowskie w zwiększaniu bezpieczeństwa miejskiego i regionalnego za pośrednictwem Europejskiego Funduszu Rozwoju Regionalnego**.**

Silniejsze podstawy edukacyjne i umiejętności są fundamentem odpornych i spójnych społeczeństw. Za pośrednictwem **unii umiejętności** i **planu działania na rzecz integracji i włączenia społecznego** Unia będzie pracować nad tym, by pomóc obywatelom zwiększać ich odporność na dezinformację, radykalizację postaw i werbowanie do grup przestępczych.

Jednym z głównych celów UE jest ochrona dzieci przed wszelkimi formami przemocy, w tym przestępczością, przemocą fizyczną lub psychiczną, zarówno w internecie, jak i poza nim. Aby zaspokoić specjalne potrzeby grup szczególnie wrażliwych, takich jak dzieci, które są coraz bardziej narażone na werbowanie i radykalizację postaw, nagabywanie dla celów seksualnych i niegodziwe traktowanie w celach seksualnych, cyberszykanowanie, dezinformację i inne zagrożenia, UE opracuje **plan działania na rzecz ochrony dzieci przed przestępczością**, obejmujący wymiary online i offline. W planie tym określone zostanie spójne i skoordynowane podejście oparte na dostępnych ramach i narzędziach, w tym na przyszłym Unijnym Centrum

[60] https://www.eucpn.org/.

ds. Zapobiegania Niegodziwemu Traktowaniu Dzieci w Celach Seksualnych i Jego Zwalczania, oraz na doświadczeniach innych organów i agencji UE, a także zaproponowane zostaną dalsze działania w obszarach, w których nadal występują luki.

Likwidacja siatek przestępczych i czynników im sprzyjających

Należy zintensyfikować walkę z siatkami przestępczymi wysokiego ryzyka, przywódcami oraz czynnikami umożliwiającymi funkcjonowanie tych siatek. Chociaż niedawne sukcesy są godne uwagi[61], przestarzałe przepisy i niespójne definicje siatek przestępczych utrudniają skuteczną reakcję wymiaru sprawiedliwości w sprawach karnych i współpracę transgraniczną. Komisja dokona przeglądu przestarzałych przepisów w tej dziedzinie, proponując odnowione **ramy prawne dotyczące przestępczości zorganizowanej**, które pozwolą wzmocnić reakcję.

Egzekwowanie przepisów na szczeblu administracyjnym może uzupełniać egzekwowanie prawa w celu osiągnięcia szybszych wyników – jak wykazała Prokuratura Europejska i Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) w zwalczaniu **transgranicznych nadużyć finansowych i przestępstw przeciwko interesom finansowym UE**. Oszuści wyłudzający dotacje koncentrują się na takich sektorach, jak energia ze źródeł odnawialnych, programy badawcze i sektor rolny[62]. Komisja zbada sposoby koordynacji wykorzystania narzędzi karnych i administracyjnych, zacieśniając współpracę z Europolem, Eurojustem i EPPO. Komisja będzie również nadal wspierać szersze stosowanie **podejścia administracyjnego** w celu wzmocnienia pozycji władz lokalnych i innych organów administracyjnych, aby przerwać infiltrację przestępczą[63].

UE pracuje nad wzmocnieniem swoich ram prawnych w zakresie zwalczania **korupcji**[64]. Parlament Europejski i Rada powinny szybko zakończyć negocjacje w sprawie zaktualizowanych ram antykorupcyjnych zaproponowanych przez Komisję. Komisja przedstawi unijną strategię antykorupcyjną, której celem będzie wspieranie uczciwości i wzmocnienie koordynacji między wszystkimi właściwymi organami i zainteresowanymi stronami w tej dziedzinie.

Broń palna jest kluczowym czynnikiem powodującym wzrost przemocy popełnianej przez zorganizowane grupy przestępcze. Komisja zaproponuje wspólne normy prawa karnego dotyczące nielegalnego handlu bronią palną. Nowy **plan działania UE w sprawie nielegalnego handlu bronią palną** skoncentruje się na ochronie legalnego rynku, ograniczaniu działalności przestępczej w oparciu o lepsze dane wywiadowcze i zacieśnianiu współpracy międzynarodowej, ze szczególnym uwzględnieniem Ukrainy i Bałkanów Zachodnich.

Nielegalnie sprzedawane materiały pirotechniczne wykorzystywane w przestępstwach wymagają środków mających na celu poprawę prewencji i identyfikowalności. Komisja dokonuje obecnie oceny dyrektywy w sprawie wyrobów pirotechnicznych i rozważy również **sankcje karne za nielegalny handel materiałami pirotechnicznymi**.

[61] W tym niedawne sprawy EMPACT.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania korupcji, zastępującej decyzję ramową Rady 2003/568/WSiSW oraz Konwencję w sprawie zwalczania korupcji urzędników Wspólnot Europejskich i urzędników państw członkowskich Unii Europejskiej oraz zmieniającej dyrektywę Parlamentu Europejskiego i Rady (UE) 2017/1371, COM(2023) 234 final, Bruksela, 3 maja 2023 r.

Podążanie śladem pieniędzy

Monitorowanie przepływów pieniężnych ma kluczowe znaczenie dla zwalczania przestępczości zorganizowanej i terroryzmu, ale nadal jest bardzo trudne. Związek między przestępczością zorganizowaną a przepływami pieniężnymi wymaga intensywnych i połączonych wysiłków w celu powstrzymania dostępu siatek przestępczych do źródeł finansowania oraz lepszej ochrony obywateli, przedsiębiorstw i budżetów publicznych.

UE zintensyfikowała swoje wysiłki dzięki nowym przepisom dotyczącym przeciwdziałania praniu pieniędzy, w tym ustanowieniu unijnego **Urzędu ds. Przeciwdziałania Praniu Pieniędzy (AMLA)**[65]. Współpraca między AMLA, OLAF-em, EPPO, Eurojustem i Europolem ma zasadnicze znaczenie dla prowadzenia skutecznych dochodzeń finansowych. Komisja będzie wspierać tworzenie **partnerstw**, zarówno ułatwiających współpracę międzyagencyjną, jak i angażujących sektor prywatny.

Aby zlikwidować finansowe motywy przestępczości zorganizowanej, zasadnicze znaczenie ma zajmowanie mienia i konfiskata korzyści pochodzących z działalności przestępczej. Niedawno przyjęte bardziej rygorystyczne przepisy dotyczące **odzyskiwania i konfiskaty mienia**[66] powinny zostać niezwłocznie transponowane przez państwa członkowskie, a ich potencjał w pełni wykorzystany. Zwalczanie równoległych systemów finansowych obchodzących unijne ramy przeciwdziałania praniu pieniędzy, w tym systemów opartych na kryptowalutach, również wymaga innowacyjnych działań, wymiany najlepszych praktyk między państwami członkowskimi oraz zwiększonego wsparcia ze strony Europolu i Eurojustu. Komisja zbada wykonalność nowego ogólnounijnego systemu śledzenia zysków z przestępczości zorganizowanej i finansowania terroryzmu, a także będzie zachęcać do terminowego i rozszerzonego przepływu informacji z **jednostek analityki finansowej** do organów ścigania. Komisja zbada sposoby wyeliminowania luk prawnych, będzie wspierać państwa członkowskie w budowaniu zdolności i będzie kontynuować prace nad zacieśnieniem współpracy z państwami trzecimi wykorzystywanymi przez przestępców do prowadzenia podziemnych operacji bankowych.

Zwalczanie poważnych przestępstw

Walka z poważnymi przestępstwami – oprócz rozbijania siatek przestępczych – wymaga ukierunkowanych wysiłków. Aby zwiększyć zdolność Unii do zwalczania **oszustw internetowych**, które powodują bardzo poważne szkody finansowe[67], Komisja będzie wspierać środki zapobiegawcze i skuteczniejsze działania organów ścigania oraz będzie współpracować z państwami członkowskimi i zainteresowanymi stronami w celu wspierania i ochrony ofiar, w tym poprzez pomoc w odzyskiwaniu ich środków finansowych. Wysiłki te zostaną sformalizowane w **planie działania w sprawie oszustw internetowych**.

Opierając się na strategii UE na lata 2020–2025 na rzecz zwalczania **niegodziwego traktowania dzieci w celach seksualnych**[68], Komisja będzie wspierać współprawodawców w sfinalizowaniu dwóch wniosków ustawodawczych[69] mających na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych w internecie i zwalczanie tego zjawiska oraz zwiększenie skuteczności działań organów ścigania przeciwko niegodziwemu traktowaniu dzieci w celach seksualnych i wykorzystywaniu seksualnemu dzieci. Z uwagi na fakt, że do kwietnia 2026 r. obowiązują przepisy przejściowe, konieczne jest ustanowienie

[65] https://www.amla.europa.eu/index_pl.

[66] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1260 z dnia 24 kwietnia 2024 r. w sprawie odzyskiwania i konfiskaty mienia, Dz.U. L, 2024/1260, 2.5.2024.

[67] Global Anti-Scam Report 2024 [Światowe sprawozdanie na temat walki z oszustwami z 2024 r.].

[68] COM(2020) 607 final

[69] COM(2022) 209 final i COM(2024) 60 final.

stałych ram prawnych, a Komisja zachęca współprawodawców do rozpoczęcia negocjacji w sprawie projektu rozporządzenia ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i zwalczanie tego zjawiska. Zachęca się również współprawodawców do poczynienia postępów w negocjacjach dotyczących dyrektywy w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, która ustanowi normy minimalne dotyczące definicji przestępstw i kar w dziedzinie wykorzystywania seksualnego dzieci.

Połowa najniebezpieczniejszych siatek przestępczych w UE jest zamieszana w agresywny **nielegalny obrót środkami odurzającymi**. Chociaż UE zintensyfikowała ostatnio walkę z tym przestępstwem[70], zwłaszcza poprzez rozszerzenie mandatu **Agencji UE ds. Narkotyków**, konieczne są dalsze działania. Komisja będzie ściśle współpracować z państwami członkowskimi w celu zaproponowania nowej **strategii UE w dziedzinie narkotyków**. Dokona również przeglądu **ram prawnych dotyczących prekursorów narkotyków** i zaproponuje **europejski plan działania przeciwko nielegalnemu obrotowi środkami odurzającymi**, aby zakłócić szlaki i modele biznesowe**. Partnerstwo publiczno-prywatne sojuszu portów europejskich** na rzecz wzmocnionej ochrony portów zostanie rozszerzone na mniejsze porty i porty śródlądowe oraz zapewni egzekwowanie przepisów dotyczących bezpieczeństwa morskiego. Dostrzegając poważne lokalne skutki nielegalnego obrotu środkami odurzającymi, Komisja będzie nadal wspierać zrównoważoną, opartą na dowodach i multidyscyplinarną politykę antynarkotykową, a także gotowość na nagłe napływy narkotyków, zwłaszcza syntetycznych opioidów.

Aby zwalczać wykorzystywanie ludzi, UE przyjęła nowe przepisy[71] i wprowadzi **odnowioną strategię UE w zakresie zwalczania handlu ludźmi** (2026–2030), obejmującą wszystkie etapy od zapobiegania po ściganie, ze szczególnym uwzględnieniem wsparcia dla ofiar zarówno na szczeblu unijnym, jak i międzynarodowym.

W walce z **przemytem migrantów** Komisja będzie przewodzić wysiłkom wraz z kluczowymi partnerami za pośrednictwem nowego światowego sojuszu na rzecz przeciwdziałania przemytowi migrantów, we współpracy z Europolem, Eurojustem i Fronteksem, w tym w wymiarze online. Wnioski Komisji dotyczące przeciwdziałania przemytowi[72] powinny zostać niezwłocznie przyjęte i wdrożone. Ponadto Komisja, po przyjęciu **zestawu narzędzi dotyczącego przewoźników**[73], zwiększyła kontakty z zagranicznymi organami i przewoźnikami i będzie nadal współpracować z przemysłem lotniczym i organizacjami lotnictwa cywilnego[74] w celu szerzenia wiedzy na temat przemytu migrantów drogą powietrzną[75].

Przestępstwa przeciwko środowisku zagrażają środowisku, zdrowiu publicznemu i gospodarce w perspektywie długoterminowej. Komisja będzie wspierać państwa

[70] COM(2023) 641 final.
[71] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1712 z dnia 13 czerwca 2024 r. w sprawie zmiany dyrektywy 2011/36/UE w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, Dz.U. L, 2024/1712, 24.6.2024.
[72] COM(2023) 755 final i COM(2023) 754 final.
[73] Zestaw narzędzi dotyczących wykorzystania komercyjnych środków transportu w celu ułatwienia nielegalnej migracji do UE.
[74] W tym z Organizacją Międzynarodowego Lotnictwa Cywilnego (ICAO).
[75] Komisja będzie również wspierać sfinalizowanie rozporządzenia w sprawie środków wobec przewoźników, którzy ułatwiają handel ludźmi lub przemyt migrantów lub zajmują się takim handlem lub przemytem, COM(2021) 753 final.

członkowskie we wdrażaniu dyrektywy w sprawie przestępstw przeciwko środowisku[76] oraz wzmacniać sieci operacyjne i działania w tej dziedzinie[77]. Zasadnicze znaczenie ma stanowcze egzekwowanie prawa. Ponadto niedawno przyjęta Konwencja Rady Europy o ochronie środowiska poprzez prawo karne[78] pomoże zapewnić zdecydowane i porównywalne wysiłki na rzecz zwalczania przestępstw przeciwko środowisku, zarówno w Europie, jak i poza nią.

Reakcja wymiaru sprawiedliwości w sprawach karnych

Przestępczość i terroryzm mogą mieć wpływ na wszystkich, co sprawia, że zasadnicze znaczenie ma wspieranie i ochrona praw **ofiar**, która pozwoli ograniczyć szkody i zwiększyć ogólnie pojęte bezpieczeństwo i zaufanie do władz. Opierając się na dyrektywie o prawach ofiar, Komisja wprowadzi nową **Strategię UE w zakresie praw ofiar**.

Unijne systemy wymiaru sprawiedliwości w sprawach karnych potrzebują skutecznych narzędzi, aby stawić czoła pojawiającym się zagrożeniom. Aby to osiągnąć, Komisja uruchomiła **forum wysokiego szczebla w sprawie przyszłości unijnego wymiaru sprawiedliwości w sprawach karnych**. Forum to skupia państwa członkowskie, Parlament Europejski, agencje i organy UE oraz inne odpowiednie zainteresowane strony. Jego celem jest omówienie sposobów zapewnienia, aby nasze systemy wymiaru sprawiedliwości w sprawach karnych pozostały skuteczne, sprawiedliwe i odporne w obliczu zmieniających się wyzwań, przy jednoczesnym wzmocnieniu współpracy sądowej i zwiększeniu wzajemnego zaufania, w tym przez cyfryzację[79].

Kluczowe działania

Komisja:

- **przedstawi w 2026 r. wniosek ustawodawczy w sprawie zmodernizowanych przepisów dotyczących przestępczości zorganizowanej;**
- **przedstawi w 2025 r. wniosek ustawodawczy w sprawie zmiany ram prawnych dotyczących prekursorów narkotyków;**
- **przedstawi w 2025 r. wniosek ustawodawczy w sprawie wspólnych norm prawa karnego dotyczących nielegalnego handlu bronią palną;**
- **oceni potrzebę zmiany dyrektyw w sprawie wyrobów pirotechnicznych i materiałów wybuchowych przeznaczonych do użytku cywilnego;**
- **oceni potrzebę dalszego wzmocnienia europejskiego nakazu dochodzeniowego i europejskiego nakazu aresztowania;**
- **przedstawi w 2026 r. nową strategię UE w zakresie zwalczania handlu ludźmi;**
- **przedstawi w 2026 r. nową Strategię UE w zakresie praw ofiar;**
- **przedstawi do 2027 r. plan działania UE na rzecz ochrony dzieci przed przestępczością;**
- **przedstawi w 2025 r. europejski plan działania przeciwko nielegalnemu obrotowi środkami odurzającymi;**

[76] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1203 z dnia 11 kwietnia 2024 r. w sprawie ochrony środowiska poprzez prawo karne, Dz.U. L, 2024/1203, 30.4.2024.

[77] Europejska Sieć Wdrażania i Egzekwowania Prawa Ochrony Środowiska (IMPEL), Europejska Sieć Prokuratorów ds. Przestępczości przeciwko Środowisku (ENPE), EnviCrimeNet i Europejskie Forum Sędziów na Rzecz Środowiska (EUFJE).

[78] Komitet ekspertów ds. ochrony środowiska poprzez prawo karne (PC-ENV) – Europejski Komitet Problematyki Przestępczości.

[79] W szczególności poprzez ustanowienie elektronicznej wymiany informacji z dziedziny e-sprawiedliwości (system eCODEX) oraz europejskiego systemu przekazywania informacji z rejestrów karnych – obywatele państw trzecich (ECRIS-TCN).

- **przedstawi w 2026 r. plan działania UE w sprawie nielegalnego handlu bronią palną;**
- **począwszy od 2025 r. będzie sukcesywnie rozszerzać sojusz portów europejskich;**
- **przyjmie w 2026 r. określone w akcie o usługach cyfrowych wytyczne dotyczące ochrony małoletnich;**
- **przedstawi w 2026 r. plan działania UE przeciwko cyberszykanowaniu.**

Państwa członkowskie wzywa się do:

- **pełnej transpozycji nowych przepisów dotyczących odzyskiwania i konfiskaty mienia do końca 2026 r. i pełnego wykorzystania ich potencjału;**
- **wdrożenia podejścia administracyjnego w walce z infiltracją przestępczą;**
- **ustanowienia partnerstw publiczno-prywatnych na rzecz przeciwdziałania praniu pieniędzy;**
- **transpozycji i pełnego wdrożenia dyrektywy w sprawie zapobiegania i zwalczania przemocy wobec kobiet i przemocy domowej.**

Parlament Europejski i Radę wzywa się do:

- **poczynienia postępów w negocjacjach dotyczących rozporządzenia ustanawiającego przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i zwalczanie tego zjawiska oraz dyrektywy w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych;**
- **zakończenia negocjacji dotyczących dyrektywy w sprawie zwalczania korupcji.**

6. Zwalczanie terroryzmu i brutalnego ekstremizmu

Wprowadzimy kompleksowy plan w dziedzinie zwalczania terroryzmu, aby zapobiegać radykalizacji postaw, zabezpieczać przestrzeń internetową i publiczną, ograniczać kanały finansowania i reagować na ataki, gdy do nich dojdzie.

Zagrożenie terrorystyczne w UE jest nadal wysokie. Jest ono ściśle powiązane ze skutkami ubocznymi wydarzeń geopolitycznych, nowymi technologiami i nowymi sposobami finansowania terroryzmu. Musimy zadbać o to, by UE była dobrze przygotowana do przewidywania zagrożeń, zapobiegania radykalizacji postaw (zarówno w internecie, jak i poza nim), do ochrony obywateli i przestrzeni publicznej przed atakami oraz do skutecznego reagowania na ataki, gdy do nich dojdzie. W 2025 r. przedstawiona zostanie **nowa unijna agenda na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk**, która określi przyszłe działania UE. Zgodnie z tą nową agendą UE i Bałkany Zachodnie podpiszą w 2025 r. nowy **wspólny plan działania** na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk.

Zapobieganie radykalizacji i ochrona osób w internecie

Podobnie jak w przypadku zwalczania przestępczości zorganizowanej przeciwdziałanie terroryzmowi i brutalnemu ekstremizmowi zaczyna się od **eliminowania jego pierwotnych przyczyn**. Swoje wsparcie dla praktyków i decydentów politycznych zwiększy **unijne centrum wiedzy w zakresie zapobiegania radykalizacji postaw** dzięki nowemu **kompleksowemu zestawowi narzędzi prewencyjnych**, aby umożliwić wczesną identyfikację i interwencje ukierunkowane na osoby najbardziej narażone, w szczególności na małoletnich.

Do radykalizacji często dochodzi w zakładach karnych – Komisja wyda nowe zalecenia, aby wspierać państwa członkowskie w rozwiązywaniu tego problemu.

Terroryści i brutalni ekstremiści wykorzystują platformy internetowe do rozpowszechniania terrorystycznych i szkodliwych treści, gromadzenia funduszy i werbowania. Podatni użytkownicy, zwłaszcza małoletni, ulegają radykalizacji postaw w internecie w alarmującym tempie. Kluczową rolę w przeciwdziałaniu rozprzestrzenianiu się w internecie treści o charakterze terrorystycznym odgrywa **rozporządzenie w sprawie treści o charakterze terrorystycznym w internecie**, umożliwiając szybkie usuwanie najbardziej odrażających i niebezpiecznych materiałów[80]. Komisja dokonuje obecnie oceny jego funkcjonowania i oceni, w jaki sposób najlepiej wzmocnić te ramy.

Unijny protokół kryzysowy dotyczący wspólnej i szybkiej reakcji organów ścigania i branży technologicznej w związku z atakiem terrorystycznym zostanie zmieniony, aby zapewnić skalowalność i elastyczność reagowania na rosnący internetowy wymiar ataków terrorystycznych. Forum UE ds. Internetu będzie nadal głównym sposobem dobrowolnej współpracy z branżą technologiczną w celu zwalczania terrorystycznych i szkodliwych treści w internecie. Ponadto Komisja angażuje się w inicjatywy międzynarodowe, takie jak fundacja Christchurch Call i Globalne Internetowe Forum Przeciwdziałania Terroryzmowi (GIFCT).

Przeciwdziałanie finansowaniu terroryzmu

Terroryści finansują swoją działalność za pomocą kampanii finansowania społecznościowego, kryptoaktywów, neobanków lub platform płatności internetowych. Organy ścigania muszą wykrywać i badać te przepływy finansowe. Wymaga to środków, narzędzi i wiedzy specjalistycznej. Kluczową rolę odgrywa **sieć urzędników prowadzących śledztwa finansowe w kontekście zwalczania terroryzmu**. Komisja zbada możliwość utworzenia **nowego ogólnounijnego systemu śledzenia finansowania terroryzmu** obejmującego transakcje wewnątrzunijne i SEPA, transfery kryptoaktywów, płatności online i przelewy bankowe, uzupełniającego umowę w sprawie Programu UE–USA śledzenia środków finansowych należących do terrorystów (TFTP).

Należy chronić budżet UE przed **nadużyciami w celu wspierania radykalnych/ekstremistycznych poglądów** w państwach członkowskich. Zmienione **rozporządzenie finansowe** przewiduje obecnie, że wyrok skazujący za „podżeganie do dyskryminacji, nienawiści lub przemocy", może być podstawą wykluczenia z finansowania unijnego. Komisja będzie nadal badać najlepszy sposób pełnego wykorzystania tego zestawu narzędzi, w tym przy wyborze potencjalnych beneficjentów. Ochrona budżetu UE zależy również od ścisłej współpracy i wymiany informacji z organami krajowymi, agencjami i organami UE.

Ochrona przed atakami

Oprócz inwestycji w zapobieganie radykalizacji postaw ważnym elementem ochrony obywateli jest ograniczenie środków, za pomocą których terroryści i przestępcy mogą przeprowadzać ataki. Konieczne są działania zarówno w odniesieniu do narzędzi, z których korzystają terroryści, jak i ochrony celów zagrożonych atakiem.

Oprócz działań dotyczących broni palnej Komisja dokona również **przeglądu przepisów** dotyczących **prekursorów materiałów wybuchowych** w celu uwzględnienia chemikaliów wysokiego ryzyka. Najczęstszym celem ataków terrorystycznych, zwłaszcza w przypadku

[80] Do 31 grudnia 2024 r. wydano 1 426 nakazów usunięcia treści o charakterze terrorystycznym lub zablokowania dostępu do nich, z których zdecydowana większość dotyczyła treści o charakterze terrorystycznym związanych z dżihadem, ale także prawicowych treści o charakterze terrorystycznym.

sprawców działających w pojedynkę, pozostaje **przestrzeń publiczna**. Aby chronić obywateli przed przemocą, **program doradców UE ds. zapewniania bezpieczeństwa** zostanie rozwinięty w celu przeprowadzania ocen podatności przestrzeni publicznych, infrastruktury krytycznej i wydarzeń wysokiego ryzyka, na wniosek państw członkowskich i finansowany z budżetu UE w ramach Funduszu Bezpieczeństwa Wewnętrznego. UE będzie dążyć do zwiększenia dostępnych środków finansowych na ochronę przestrzeni publicznej. Komisja oferuje wsparcie organom państw członkowskich i podmiotom prywatnym za pośrednictwem specjalnych wytycznych i narzędzi, takich jak centrum wiedzy na temat ochrony przestrzeni publicznej[81], a od 2020 r. udostępniono już 70 mln EUR na wsparcie ochrony przestrzeni publicznej.

Komisja zbada również wprowadzenie dla organizacji wymogów dotyczących rozważenia lub zastosowania środków bezpieczeństwa w publicznie dostępnych miejscach poprzez współpracę z władzami lokalnymi i partnerami prywatnymi.

Ze względu na oczywiste zagrożenia Komisja w swoich działaniach na rzecz ochrony społeczności żydowskiej będzie nadal kierować się **Strategią UE w sprawie zwalczania antysemityzmu i wspierania życia żydowskiego (2021–2030)**. Komisja zapewni również, by istniały odpowiednie narzędzia wspierające państwa członkowskie w zwalczaniu **nienawiści antymuzułmańskiej**.

Coraz większe zagrożenie bezpieczeństwa stanowi wykorzystywanie **bezzałogowych statków powietrznych** do szpiegostwa i ataków. Komisja opracuje **zharmonizowaną metodykę testowania systemów przeciwdziałania bezzałogowym statkom powietrznym**, utworzy **centrum doskonałości na rzecz przeciwdziałania bezzałogowym statkom powietrznym** i oceni potrzebę harmonizacji przepisów i procedur państw członkowskich[82].

Zagraniczni bojownicy terrorystyczni

Aby zidentyfikować zagranicznych bojowników terrorystycznych powracających lub wjeżdżających na granice zewnętrzne UE, potrzebne są dane dotyczące osób stwarzających zagrożenie terrorystyczne. W tym celu Komisja wraz z Europolem zacieśni **współpracę z kluczowymi państwami trzecimi w celu uzyskania danych biograficznych i biometrycznych dotyczących osób mogących stanowić zagrożenie terrorystyczne**, w tym zagranicznych bojowników terrorystycznych. Dane te można następnie wprowadzić do Systemu Informacyjnego Schengen w pełnej zgodności z obowiązującymi unijnymi i krajowymi ramami prawnymi. Dlatego niezwykle ważne jest, aby państwa członkowskie korzystały ze wszystkich istniejących narzędzi. Obejmuje to wprowadzanie wszystkich istotnych informacji do **SIS**, usprawnienie kontroli biometrycznych i przeprowadzanie obowiązkowych systematycznych kontroli wszystkich osób na granicach zewnętrznych UE[83]. Ponadto **wspólne wskaźniki ryzyka** opracowane przez Frontex będą nadal wspierać organy kontroli granicznej państw członkowskich w identyfikowaniu i ocenie ryzyka podejrzanych podróży potencjalnych zagranicznych bojowników terrorystycznych.

Ponadto w celu zapewnienia, aby państwa członkowskie utrzymały dostęp do **dowodów z pola walki** zebranych przez zespół dochodzeniowo-śledczy ONZ na rzecz promowania rozliczalności za zbrodnie popełnione przez Daisz/ISIL na potrzeby ścigania zagranicznych bojowników terrorystycznych, Komisja wraz z Eurojustem oceni możliwość przechowywania tych dowodów w prowadzonej przez Eurojust bazie dowodów najpoważniejszych zbrodni wagi

[81] Centrum wiedzy na temat ochrony przestrzeni publicznej.
[82] Zgodnie z zestawem kluczowych działań określonym w komunikacie dotyczącym przeciwdziałania potencjalnym zagrożeniom stwarzanym przez bezzałogowe statki powietrzne z 2023 r., COM(2023) 659 final.
[83] Przy zapewnieniu pełnej zgodności z kodeksem granicznym Schengen i rozporządzeniem w sprawie kontroli przesiewowej.

międzynarodowej. Ponadto nowy europejski **sądowy rejestr antyterrorystyczny** będzie nadal wspierać organy wymiaru sprawiedliwości państw członkowskich w szybkim identyfikowaniu powiązań transgranicznych w sprawach dotyczących terroryzmu.

Kluczowe działania

Komisja:

- **przyjmie w 2025 r. nową unijną agendę na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk;**
- **podpisze w 2025 r. z Bałkanami Zachodnimi nowy wspólny plan działania na rzecz zapobiegania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk;**
- **opracuje wraz z unijnym centrum wiedzy nowy kompleksowy zestaw narzędzi prewencyjnych;**
- **oceni w 2026 r. stosowanie rozporządzenia w sprawie treści o charakterze terrorystycznym w internecie;**
- **zmieni w 2025 r. unijny protokół kryzysowy;**
- **przedstawi w 2026 r. wniosek ustawodawczy dotyczący zmiany rozporządzenia w sprawie wprowadzania do obrotu i używania prekursorów materiałów wybuchowych;**
- **zbada wykonalność nowego ogólnounijnego systemu śledzenia finansowania terroryzmu.**

Państwa członkowskie wzywa się do:

- **usprawnienia kontroli biometrycznych i przeprowadzania obowiązkowych systematycznych kontroli na granicach zewnętrznych UE;**
- **pełnego wykorzystania europejskiego sądowego rejestru antyterrorystycznego.**

7. Silna pozycja UE na arenie światowej w dziedzinie bezpieczeństwa

Aby zwiększyć bezpieczeństwo UE, zacieśnimy współpracę operacyjną poprzez partnerstwa z kluczowymi regionami, takimi jak nasi partnerzy objęci procesem rozszerzenia i polityką sąsiedztwa, Ameryka Łacińska i region Morza Śródziemnego. Interesy UE w zakresie bezpieczeństwa zostaną uwzględnione we współpracy międzynarodowej, w tym poprzez wykorzystanie narzędzi i instrumentów UE.

Ostatnie lata pokazały ścisły związek między bezpieczeństwem zewnętrznym i wewnętrznym UE. Rosyjska wojna napastnicza przeciwko Ukrainie, konflikt w Strefie Gazy, sytuacja w Syrii i pojawiające się konflikty na całym świecie miały poważne skutki uboczne dla bezpieczeństwa wewnętrznego UE. Aby przeciwdziałać wpływowi globalnej niestabilności na bezpieczeństwo wewnętrzne, **UE musi aktywnie bronić swoich interesów w zakresie bezpieczeństwa** poprzez przeciwdziałanie zagrożeniom zewnętrznym, zakłócanie szlaków przemytu oraz ochronę korytarzy o znaczeniu strategicznym, takich jak szlaki handlowe. Jednocześnie UE będzie nadal silnym sojusznikiem krajów partnerskich, współpracując na rzecz zwiększenia globalnego bezpieczeństwa i budowania wzajemnej odporności na zagrożenia.

W ostatnich latach UE podjęła istotne kroki w celu zacieśnienia współpracy w dziedzinie bezpieczeństwa. Zawarła umowy operacyjne dotyczące egzekwowania prawa i współpracy sądowej, a także inne rodzaje porozumień z krajami partnerskimi. Aktywnie dąży do zawierania dodatkowych umów międzynarodowych, zgodnie z wytycznymi negocjacyjnymi Rady, oraz podejmowania inicjatyw na rzecz budowania zdolności, wspieranych przez agencje

i organy UE. Kluczowe znaczenie dla wzmocnienia bezpieczeństwa z krajami partnerskimi ma również instrument ISWMR – „Globalny wymiar Europy".

Podstawą wzmocnienia światowego bezpieczeństwa jest **wielostronny porządek oparty na zasadach**. Zasadnicze znaczenie dla wzmocnienia tych wysiłków mają dialogi na temat bezpieczeństwa, w tym dialogi tematyczne. Kluczowe znaczenie dla opracowania skutecznych rozwiązań w zakresie bezpieczeństwa ma wdrożenie **Strategicznego kompasu na rzecz bezpieczeństwa i obrony**, wraz z ramami współpracy dwustronnej i wielostronnej, takimi jak układy o stabilizacji i stowarzyszeniu oraz układy o stowarzyszeniu, a także współpraca z organizacjami takimi jak ONZ i NATO. UE będzie nadal odgrywać rolę na forach wielostronnych[84] i zacieśniać współpracę z odpowiednimi organizacjami i ramami międzynarodowymi i regionalnymi, w tym z NATO, Organizacją Narodów Zjednoczonych, Radą Europy, Interpolem, grupą G-7, OBWE i społeczeństwem obywatelskim.

Współpraca regionalna

Priorytetem jest kontynuowanie niezachwianego wsparcia UE dla **Ukrainy** oraz wzmocnienie bezpieczeństwa i odporności **krajów objętych procesem rozszerzenia UE**, co jest koniecznością ze względów politycznych i geostrategicznych. Wspieranie bezpieczeństwa UE powinno iść w parze z **przyspieszoną integracją krajów kandydujących** z **unijną architekturą bezpieczeństwa**, równolegle z konsolidacją ich współpracy regionalnej. Komisja wykorzysta unijną politykę rozszerzenia do wspierania zdolności krajów kandydujących do UE i potencjalnych krajów kandydujących do reagowania na zagrożenia, do zacieśnienia współpracy operacyjnej i wymiany informacji oraz do zapewnienia zgodności z unijnymi zasadami, prawodawstwem i narzędziami. Kluczowe znaczenie dla wzmocnienia bezpieczeństwa zarówno w krajach kandydujących, jak i potencjalnych krajach kandydujących ma Instrument Pomocy Przedakcesyjnej (IPA III), a także instrumenty dla Ukrainy, Mołdawii i Bałkanów Zachodnich.

UE będzie również dalej włączać **partnerów objętych polityką sąsiedztwa** do unijnej struktury bezpieczeństwa. Za pośrednictwem **nowego paktu na rzecz regionu śródziemnomorskiego** i przyszłego **strategicznego podejścia do regionu Morza Czarnego** Unia będzie dążyć do dalszego budowania współpracy regionalnej i dwustronnych kompleksowych partnerstw strategicznych mających wymiar bezpieczeństwa, w stosownych przypadkach, poprzez regularne dialogi na wysokim szczeblu dotyczące bezpieczeństwa. Wzmocniona zostanie współpraca operacyjna z Afryką Północną, **Bliskim Wschodem i Zatoką Perską**, w szczególności w zakresie zwalczania terroryzmu, przeciwdziałania praniu pieniędzy, handlu bronią palną oraz produkcji i handlu narkotykami, zwłaszcza captagonem**.**

Aby zaradzić nasilaniu się działalności terrorystycznej i przestępczej oraz jej potencjalnym skutkom ubocznym w **Afryce Subsaharyjskiej**, **zwłaszcza w Sahelu, Rogu Afryki** i **Afryce Zachodniej**, UE zwiększy wsparcie dla Unii Afrykańskiej, regionalnych wspólnot gospodarczych i krajów w regionie. Zgodnie ze strategią Unii Europejskiej w zakresie bezpieczeństwa morskiego[85] UE wzmocni współpracę w **Zatoce Gwinejskiej, na Morzu Czerwonym i na Oceanie Indyjskim** w celu zwalczania nielegalnego handlu i piractwa, wspierając współpracę wewnątrzafrykańską i regionalną, a także przy wsparciu unijnej skoordynowanej obecności na morzu (CMP) oraz Morskiego Centrum Analiz i Operacji ds. Zwalczania Narkotyków (MAOC-N).

[84] Światowe Forum na rzecz Zwalczania Terroryzmu, globalna koalicja na rzecz walki z Daisz, Globalne Internetowe Forum Przeciwdziałania Terroryzmowi (GIFCT), fundacja Christchurch Call, światowa koalicja na rzecz przeciwdziałania zagrożeniom związanym z narkotykami syntetycznymi.
[85] JOIN(2023) 8 final.

Z **Ameryką Łacińską i regionem Karaibów** UE wzmocni współpracę operacyjną w celu likwidacji i ścigania siatek przestępczych wysokiego ryzyka oraz przerwania nielegalnej działalności i szlaków nielegalnego handlu, wzmacniając ramy współpracy, takie jak UE-CLASI (Komitet Ameryki Łacińskiej ds. Bezpieczeństwa Wewnętrznego) oraz mechanizm koordynacji i współpracy UE-CELAC w zakresie środków odurzających. Wśród priorytetów znajdą się odporność węzłów logistycznych, partnerstwa i zasada podążania śladem pieniędzy. UE będzie nadal wspierać rozwój Wspólnoty Sił Policyjnych Kontynentów Amerykańskich (AMERIPOL), aby stała się regionalnym odpowiednikiem Europolu i zacieśniła współpracę sądową między państwami członkowskimi a regionem. UE będzie również prowadzić współpracę z **Azją Południową i Środkową** ukierunkowaną na wspólne zagrożenia bezpieczeństwa związane z terroryzmem, handlem nielegalnymi towarami, w tym środkami odurzającymi, handlem ludźmi i przemytem migrantów.

Ponadto UE będzie wspierać ramy współpracy regionalnej w państwach trzecich, aby dalej pomagać im w powstrzymywaniu nielegalnego handlu u źródła, zgodnie z zasadą wspólnej odpowiedzialności za cały przestępczy łańcuch dostaw. UE dołoży też wszelkich starań, aby wzmocnić bezpieczeństwo węzłów logistycznych za granicą, koordynując **wspólne inspekcje w portach państw trzecich**.

Współpraca operacyjna

Strategia Global Gateway będzie wspierać zrównoważone i wysokiej jakości projekty infrastrukturalne w sektorach cyfrowym, klimatycznym i energetycznym, w sektorach transportu, zdrowia, edukacji i badań naukowych. Komisja włączy teraz, w stosownych przypadkach, względy bezpieczeństwa do przyszłych inwestycji w ramach strategii Global Gateway. Obejmie to inicjatywy o kluczowym znaczeniu dla autonomii strategicznej UE i jej krajów partnerskich, takie jak projekty infrastrukturalne obejmujące oceny bezpieczeństwa i środki zmniejszające ryzyko.

Komisja będzie dążyć do zawarcia dalszych **porozumień między UE a państwami trzecimi w sprawie współpracy z Europolem i Eurojustem**, zwłaszcza z państwami Ameryki Łacińskiej.

Ponadto aktywny udział państw niebędących członkami UE w **EMPACT** jest jednym z najskuteczniejszych sposobów wzmocnienia współpracy operacyjnej. UE będzie nadal zachęcać państwa trzecie, w szczególności Bałkany Zachodnie, wschodnie sąsiedztwo, Afrykę Subsaharyjską, Afrykę Północną, Bliski Wschód, Amerykę Łacińską i region Karaibów, do udziału w tych ramach. Innym narzędziem służącym zacieśnieniu współpracy z państwami trzecimi w zakresie zwalczania przestępczości są operacyjne grupy zadaniowe tworzone przez państwa członkowskie, koordynowane przez Europol, w których mogą uczestniczyć państwa trzecie. Komisja zamierza również sfinalizować negocjacje w sprawie umowy międzynarodowej **między UE a Interpolem**[86], zapewniającej bardziej jednolite podejście do globalnych zagrożeń bezpieczeństwa i zwalczania przestępczości transgranicznej

Unia musi prowadzić działania w terenie w ramach podejścia „Drużyna Europy”. Kluczową rolę w zapewnianiu, aby działania zewnętrzne Unii były świadome, skoordynowane i elastyczne odgrywa wyspecjalizowany personel Unii i państw członkowskich. Aby przenieść to podejście na kolejny poziom, Komisja, wspierana przez Wysokiego Przedstawiciela do Spraw Zagranicznych i Polityki Bezpieczeństwa, wzmocni **sieci łącznikowe** i ułatwi rozmieszczenie regionalnych **oficerów łącznikowych Europolu i Eurojustu**, zgodnie z potrzebami operacyjnymi państw członkowskich.

[86] Decyzja Rady (UE) 2021/1312 z dnia 19 lipca 2021 r. i decyzja Rady (UE) 2021/1313 z dnia 19 lipca 2021 r.

UE będzie dążyć do ściślejszej współpracy operacyjnej organów ścigania i wymiaru sprawiedliwości, wspierać wymianę informacji w czasie rzeczywistym i wspólne operacje za pośrednictwem **wspólnych zespołów dochodzeniowo-śledczych** w państwach trzecich przy wsparciu ze strony Europolu i Eurojustu. Komisja będzie również wspierać państwa członkowskie w tworzeniu wspólnych **centrów syntezy informacji** skupiających ekspertów i lokalne organy ścigania w strategicznych państwach trzecich.

Narzędzia wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB)

Do lepszego identyfikowania zewnętrznych zagrożeń dla bezpieczeństwa wewnętrznego UE i przeciwdziałania tym zagrożeniom zostaną również w pełni wykorzystane, zgodnie z ich mandatami określonymi przez Radę, **misje w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO)**. Aby budować zdolności państw trzecich, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz Komisja będą wspierać działania w ramach WPBiO za pomocą specjalnych instrumentów finansowania i zbadają wszystkie odpowiednie sposoby finansowania.

Ugruntowanym narzędziem WPZiB, stosowanym również w walce z terroryzmem, są **unijne środki ograniczające**. Na podstawie propozycji Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, państw członkowskich lub Komisji Rada mogłaby ocenić, w jaki sposób można zwiększyć skuteczność, operacyjność i elastyczność istniejących autonomicznych środków ograniczających (unijnej listy terrorystów). Ponadto mogłaby rozważyć zbadanie dodatkowych środków ograniczających skierowanych przeciwko siatkom przestępczym, zgodnie z celami WPZiB.

Polityka wizowa i wymiana informacji

Polityka wizowa UE jest kluczowym narzędziem współpracy z państwami trzecimi i zabezpieczenia granic Unii poprzez kontrolowanie wjazdu do UE i określanie warunków dla tego wjazdu. Komisja w pełni włączy **względy bezpieczeństwa do polityki wizowej UE** w przyszłej strategii dotyczącej polityki wizowej UE. Komisja będzie współpracować ze współprawodawcami w celu przyjęcia wniosku dotyczącego zmiany i usprawnienia mechanizmu zawieszającego zwolnienie z obowiązku wizowego, w szczególności w odniesieniu do konkretnych przypadków nadużywania systemu bezwizowego[87]. Państwa trzecie będą zachęcane do przekazywania informacji o osobach mogących stanowić zagrożenie bezpieczeństwa. Informacje te będą następnie wprowadzane do systemów informacyjnych i baz danych UE.

Aby osiągnąć koordynację polityki i wysiłków podejmowanych na wcześniejszym etapie, odblokowując bardziej efektywną, szybką i płynną współpracę, Komisja będzie pracować nad wprowadzeniem **ustaleń dotyczących przepływu danych** i badać sposoby **usprawnienia wymiany informacji** do celów egzekwowania prawa i zarządzania granicami z zaufanymi państwami trzecimi, zgodnie z prawami podstawowymi i przepisami o ochronie danych.

Kluczowe działania

Komisja:

- **zawrze umowy międzynarodowe między UE a priorytetowymi państwami trzecimi w sprawie współpracy z Europolem i Eurojustem;**
- **będzie zachęcać kraje partnerskie do udziału w EMPACT w celu zwalczania przestępczości zorganizowanej i terroryzmu;**

[87] COM(2023) 642.

- **będzie wspierać agencje i organy UE w ustanawianiu i wzmacnianiu ustaleń roboczych z krajami partnerskimi;**
- **w większym stopniu odzwierciedli względy bezpieczeństwa w polityce wizowej UE w przyszłej strategii wizowej;**
- **wzmocni wymianę informacji z zaufanymi państwami trzecimi do celów egzekwowania prawa i zarządzania granicami.**

Komisja, we współpracy z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa:

- **w pełni wykorzysta cywilne misje w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO);**
- **skoordynuje do 2027 r. wspólne inspekcje w portach państw trzecich.**

Komisja, we współpracy z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa i państwami członkowskimi:

- **wzmocni sieci łącznikowe i współpracę w ramach podejścia „Drużyna Europy";**
- **będzie tworzyć wspólne zespoły operacyjne i centra syntezy informacji w państwach trzecich począwszy od 2025 r.**

Parlament Europejski i Radę wzywa się do:

- **zakończenia negocjacji w sprawie zmiany mechanizmu zawieszającego zwolnienie z obowiązku wizowego.**

8. Wnioski

W świecie niepewności należy zwiększyć zdolność Unii do przewidywania zagrożeń bezpieczeństwa, zapobiegania im i reagowania na nie.

Nie wystarczy tylko reagować na kryzysy w momencie ich wystąpienia. Musimy być bardziej świadomi dzięki pełnemu oglądowi zagrożeń w miarę ich rozwoju i upewnić się, że nasze narzędzia i możliwości sprostają temu zadaniu.

Kompleksowy zestaw środków opisanych w niniejszej strategii pomoże stworzyć Unię o silniejszej pozycji na świecie: Unię, która jest w stanie przewidywać, planować i zaspokajać własne potrzeby w zakresie bezpieczeństwa, skutecznie reagować na zagrożenia dla swojego bezpieczeństwa wewnętrznego i pociągać sprawców do odpowiedzialności oraz chronić swoje otwarte, wolne i zamożne społeczeństwa i demokracje.

Wymaga to zmiany sposobu myślenia o bezpieczeństwie wewnętrznym. Będziemy działać na rzecz wspierania nowej kultury bezpieczeństwa UE, w której względy bezpieczeństwa są uwzględniane we wszystkich naszych przepisach, politykach i programach – od ich powstania aż do wdrożenia. I tam, gdzie współpraca w różnych obszarach polityki pozwala nam przecierać nowe szlaki.

Nie jest to zadanie tylko jednej instytucji, rządu czy podmiotu. Jest to wspólne przedsięwzięcie Europy.