Rada
Unii Europejskiej

Bruksela, 27 maja 2022 r.
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	25 maja 2022 r.
Do:	Sekretariat Generalny Rady
Nr dok. Kom.:	COM(2022) 252 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY w sprawie czwartego sprawozdania z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa

Delegacje otrzymują w załączeniu dokument COM(2022) 252 final.

Zał.: COM(2022) 252 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 25.5.2022 r.
COM(2022) 252 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie czwartego sprawozdania z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa

I. WPROWADZENIE

Rosyjska agresja na Ukrainę zdominowała obecnie agendę bezpieczeństwa UE. Wojna ta nie tylko zagraża Ukrainie, ale ma na celu naruszenie stabilności i bezpieczeństwa na świecie. W UE stwarza ona szereg zagrożeń dla bezpieczeństwa obywateli. Istnieje nowa niepewność co do dostaw energii i innych surowców, a infrastruktura krytyczna może stać się celem cyberataków. Wewnętrzne bezpieczeństwo i ochrona UE są zagrożone potencjalnymi atakami z użyciem czynników chemicznych, biologicznych lub radiologicznych w strefie wojennej oraz wypadkami związanymi z tymi czynnikami. Podatność milionów osób, które uciekły przed wojną, na zagrożenia może zostać szybko wykorzystana przez zorganizowane grupy przestępcze poprzez handel kobietami i dziećmi, które są szczególnie narażone.

W obliczu tych nowych i potencjalnych zagrożeń UE pozostała stanowcza i zjednoczona. Chociaż wpływ wojny jest jak dotąd ograniczony głównie do terytorium Ukrainy, UE zwiększyła *czujność i koordynację* poprzez lepsze monitorowanie krajobrazu zagrożeń, a także pracowała nad wzmocnieniem odporności, aby zapewnić *gotowość*.

W Deklaracji wersalskiej przyjętej na posiedzeniu, które odbyło się 10–11 marca 2022 r.[1], przywódcy europejscy podkreślili konieczność przygotowania się na szybko pojawiające się wyzwania poprzez „zabezpieczanie się przed stale nasilającą się wojną hybrydową, wzmacnianie naszej cyberodporności, ochronę naszej infrastruktury – szczególnie naszej infrastruktury krytycznej – oraz zwalczanie dezinformacji".

Ramy unii bezpieczeństwa mają zasadnicze znaczenie dla zapewnienia bezpieczeństwa w całej UE. Cztery priorytety strategiczne określone w strategii w zakresie unii bezpieczeństwa[2] pozostają bezpośrednio związane z tym zadaniem w obecnym kontekście geopolitycznym: (i) środowisko bezpieczeństwa, które wytrzyma próbę czasu; (ii) działanie w obliczu zmieniających się zagrożeń; (iii) ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną oraz (iv) silny europejski ekosystem bezpieczeństwa. Wojna uwydatniła potrzebę pełnego wykorzystania przez UE i jej państwa członkowskie instrumentów prawnych i politycznych dostępnych już w ramach strategii w zakresie unii bezpieczeństwa, które stanowią podstawę skoordynowanego wsparcia UE dla państw członkowskich w kwestiach takich jak przestępczość zorganizowana i terroryzm, cyberbezpieczeństwo i zagrożenia hybrydowe.

Europejskie agencje działające w obszarze wymiaru sprawiedliwości i spraw wewnętrznych również zintensyfikowały swoje starania w odpowiedzi na wojnę w Ukrainie, odgrywając główną rolę w przeprowadzaniu oceny zagrożeń i wspieraniu reakcji operacyjnych[3]. Innym istotnym czynnikiem jest nieustanne wzmacnianie praktyki operacyjnej i zarządzania w strefie Schengen.

W niniejszym, czwartym sprawozdaniu z postępów prac w zakresie unii bezpieczeństwa skoncentrowano się na wydarzeniach, które miały miejsce w ciągu ostatnich kilku miesięcy po rosyjskiej agresji na Ukrainę. Przedstawiono w nim przegląd działań podjętych we wszystkich aspektach Unii Bezpieczeństwa oraz rozważono potrzeby dotyczące gotowości wynikające z potencjalnych zagrożeń bezpieczeństwa związanych z wojną w Ukrainie.

---

1 https://www.consilium.europa.eu/media/54787/20220311-versailles-declaration-pl.pdf

2 COM(2020) 605.

3 Wspólne oświadczenie unijnych agencji wymiaru sprawiedliwości i spraw wewnętrznych dotyczące Ukrainy | Agencja Unii Europejskiej ds. Azylu (europa.eu)

Informacje na temat postępu prac w zakresie innych dokumentów dotyczących unii bezpieczeństwa znajdują się w załączniku.

II. CYBERBEZPIECZEŃSTWO I INFRASTRUKTURA KRYTYCZNA

Od wybuchu wojny podmioty prywatne i organizacje przestępcze upubliczniają fakt, że podejmują działania w cyberprzestrzeni wspierające jedną lub drugą stronę konfliktu. Haktywizm[4] stanowi zagrożenie ze względu na ryzyko wystąpienia w UE skutków ubocznych dla usług krytycznych, ryzyko ataków ze strony oficjalnych sieci lub innych nieprzewidzianych skutków ubocznych. Chociaż jak dotąd wojna toczyła się głównie przy użyciu środków konwencjonalnych, a jej skutki uboczne były ograniczone, ryzyko eskalacji w tym obszarze jest realne.

W związku z tym UE zintensyfikowała koordynację i gotowość. Zagrożenia wynikające z wojny uwydatniają konieczność wypracowania kultury wymiany informacji i wiedzy fachowej między UE, państwami członkowskimi i środowiskami zajmującymi się cyberbezpieczeństwem. Obejmuje to stworzenie orientacji sytuacyjnej wspólnej dla instytucji, organów i agencji UE oraz państw członkowskich, w szczególności w odniesieniu do infrastruktury krytycznej, od której zależy sprawne funkcjonowanie rynku wewnętrznego.

Odpowiedzialność za cyberataki na Ukrainę

Same cyberataki na Ukrainę rozpoczęły się przed rosyjską agresją oraz w pierwszych dniach wojny[5] i miały na celu przejęcie kont użytkowników ukraińskiego personelu wojskowego oraz zakłócenie funkcjonowania podstawowych usług, w tym kontroli granicznej i telekomunikacji.

14 stycznia 2022 r. wysoki przedstawiciel wydał w imieniu Unii Europejskiej oświadczenie[6], w którym potępił cyberataki na Ukrainę i potwierdził jednoznaczne poparcie UE dla Ukrainy.

10 maja Unia Europejska i jej państwa członkowskie, wraz z partnerami międzynarodowymi, zdecydowanie potępiły[7] szkodliwe działania w cyberprzestrzeni przeciwko Ukrainie

[4] Najnowszym przykładem haktywizmu jest wykorzystanie „protestware" do rozprzestrzeniania złośliwego oprogramowania na rosyjskie adresy IP za pośrednictwem popularnego pakietu otwartego oprogramowania, co może spowodować zagrożenia dla łańcucha dostaw i utratę zaufania do społeczności twórców otwartego oprogramowania. Komisja wyraźnie stwierdziła, że cyberataki na Rosję (nawet te przeprowadzane w dobrej wierze) są nielegalne.

[5] Sprawozdanie specjalne Microsoft: An overview of Russia's cyberattack activity in Ukraine [Przegląd działań Rosji w zakresie cyberataków w Ukrainie]; The hybrid war in Ukraine [Wojna hybrydowa w Ukrainie] – wpis na blogu w sekcji Microsoft On the Issues.

[6] https://www.consilium.europa.eu/pl/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

[7] Rosyjskie cyberoperacje przeciwko Ukrainie: oświadczenie wysokiego przedstawiciela wydane w imieniu Unii Europejskiej – Consilium (europa.eu)

przeprowadzone 24 lutego, wymierzone w sieć satelitarną KA-SAT będącą własnością Viasat i bezpośrednio przypisały odpowiedzialność za ten atak Federacji Rosyjskiej. Cyberatak ten miał istotne konsekwencje oraz spowodował masowe przerwy i zakłócenia w komunikacji między kilkoma organami publicznymi, przedsiębiorstwami i użytkownikami w Ukrainie, a także dotknął kilka państw członkowskich UE.

Czujność i koordynacja

Od czasu rosyjskiej agresji na Ukrainę wzmożono monitorowanie sytuacji związanej z cyberbezpieczeństwem w państwach członkowskich i instytucjach Unii. ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – Europejskie Centrum ds. Walki z Cyberprzestępczością działające przy Europolu i CERT-UE – zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE – oraz Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN) przyczyniły się do zwiększenia wspólnej orientacji sytuacyjnej UE, m.in. regularnie monitorując podejrzane działania w cyberprzestrzeni, w tym w określonych sektorach, takich jak energetyka, transport i lotnictwo, oraz przedstawiły oceny służące ukierunkowaniu działań zapobiegawczych.

Zintensyfikowano również koordynację i wymianę informacji z sieciami zajmującymi się cyberbezpieczeństwem, takimi jak europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe), do której należą krajowe agencje ds. cyberbezpieczeństwa, Komisja i ENISA. Aby odzwierciedlić to podejście wewnątrz instytucji UE, mechanizm koordynujący – grupa zadaniowa ds. kryzysów cyberbezpieczeństwa – umożliwia wymianę informacji między wszystkimi odpowiednimi służbami, organami i agencjami, takimi jak ENISA, Europejskie Centrum ds. Walki z Cyberprzestępczością działające przy Europolu oraz CERT-UE. Niezbędne są nieustanne starania, aby zapewnić kanały komunikacji między podmiotami ze szczebla politycznego, operacyjnego i technicznego, a także zacieśnić współpracę z siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Europol uruchomił również protokół działań UE w zakresie egzekwowania prawa w sytuacjach kryzysowych, który umożliwia wzmocnione monitorowanie zagrożeń cyberbezpieczeństwa i wymianę informacji między wieloma zainteresowanymi stronami z myślą o stworzeniu kompleksowego obrazu wywiadu cybernetycznego.

Poza zagrożeniami cyberbezpieczeństwa państwa członkowskie, ESDZ i służby Komisji wzmogły czujność w odniesieniu do narażenia infrastruktury krytycznej na inne niż cybernetyczne, fizyczne zagrożenia. Infrastruktura krytyczna i obsługujące ją podmioty mogą być narażone na zagrożenia fizyczne, takie jak sabotaż ze strony państwa lub podmiotów sponsorowanych przez państwo w ramach ewentualnych środków odwetowych wymierzonych w UE.

Gotowość

Gotowość w obszarze cyberbezpieczeństwa i bezpieczeństwa infrastruktury krytycznej jest ważniejsza niż kiedykolwiek, biorąc pod uwagę zwiększone narażenie Europy na nagromadzenie zagrożeń w związku z wojną. Starania na rzecz zwiększenia gotowości obejmowały szereg działań bezpośrednich, w tym działania przewidziane jeszcze przed

rosyjską agresją na Ukrainę. Do działań tych należą ćwiczenia, wytyczne, środki legislacyjne, zwiększanie odporności w sektorach krytycznych oraz współpraca z partnerami.

Francuska prezydencja w Radzie Unii Europejskiej wraz z Europejską Służbą Działań Zewnętrznych (ESDZ) i Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) zorganizowała na początku 2022 r. oparte na scenariuszu ćwiczenie pod nazwą EU CyCLES (Cyber Crisis Linking Exercise on Solidarity), którego celem było zwiększenie świadomości na szczeblu politycznym oraz zacieśnienie współpracy między podmiotami szczebla operacyjnego i politycznego na wypadek cyberataku na dużą skalę.

ENISA i CERT-UE opublikowali w lutym **wytyczne** dotyczące sposobów zwiększenia odporności i gotowości w UE[8]. W wytycznych tych zachęca się wszystkie organizacje sektora publicznego i prywatnego w UE do przyjęcia minimalnego zbioru najlepszych praktyk w zakresie cyberbezpieczeństwa z myślą o znacznej poprawie kultury cyberbezpieczeństwa. W marcu CERT-UE opublikował przy wsparciu ENISA[9] dalsze wytyczne techniczne, a także wytyczne dotyczące bezpieczeństwa w celu wzmocnienia konfiguracji aplikacji Signal[10], zawierające szereg praktycznych zaleceń dla organizacji służących poprawie ich podejścia do cyberbezpieczeństwa.

Inicjatywy ustawodawcze

Obecna sytuacja wskazuje na pilną konieczność **wdrożenia obowiązującego prawodawstwa** i **przyspieszenia przyjęcia oczekiwanych inicjatyw**.

Komisja wspiera państwa członkowskie we wdrażaniu **dyrektywy dotyczącej cyberbezpieczeństwa**[11], w której przewidziano wymóg dla państw członkowskich, by były odpowiednio przygotowane, np. dysponowały zespołem reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz określiły właściwe organy. Dyrektywa ta stanowi podstawę skutecznej współpracy między państwami członkowskimi. Porozumienie polityczne osiągnięte przez współprawodawców w sprawie **dyrektywy NIS 2**[12] jest kolejnym przełomem w tworzeniu solidnych unijnych ram gotowości.

NIS 2 – dalsze wzmacnianie gotowości

- W nowej dyrektywie w sprawie bezpieczeństwa sieci i systemów informatycznych zostaną usunięte niedociągnięcia z poprzedniej dyrektywy dotyczącej cyberbezpieczeństwa, aby dostosować ją do obecnych potrzeb i sprawić, by nie ulegała dezaktualizacji. Określa ona minimalne przepisy dotyczące ram regulacyjnych i ustanawia mechanizmy skutecznej współpracy między odpowiednimi organami w każdym państwie członkowskim.

[8] *Boosting your Organisation's Cyber Resilience* [Zwiększanie cyberodporności organizacji] – wspólna publikacja, 14.02.2022 r.

[9] *Security Guidance 2022-01 - Cybersecurity mitigation measures against critical threats* [Wytyczne dotyczące bezpieczeństwa 2022-01 – Środki łagodzące krytyczne zagrożenia dla cyberbezpieczeństwa]

[10] *CERT-EU Security Guidance 22-002 - Hardening Signal* [Wytyczne CERT-UE dotyczące 22-002 – wzmacnianie aplikacji Signal].

[11] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[12] COM(2020) 823.

- Rozszerzono w niej zakres przepisów, dodając nowe sektory o krytycznym znaczeniu dla gospodarki i społeczeństwa (np. sektor farmaceutyczny i sektor wyrobów medycznych czy sektor produkcji żywności). Wszystkie średnie i duże podmioty działające w sektorach objętych zakresem dyrektywy lub świadczące usługi nim objęte będą wchodziły w jej zakres. Zakresem tym objęte są również podmioty administracji publicznej w ramach instytucji rządowych na szczeblu centralnym (z wyłączeniem sądownictwa, parlamentów i banków centralnych) oraz na szczeblu regionalnym. Ponadto państwa członkowskie mogą postanowić, że dyrektywa będzie miała zastosowanie do takich podmiotów na szczeblu lokalnym.
- W dyrektywie NIS2 określone zostaną podstawy środków zarządzania ryzykiem w cyberprzestrzeni oraz formalnie ustanowiona zostanie europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa, EU-CyCLONe, która będzie wspierać skoordynowane zarządzanie cyberincydentami na dużą skalę.
- Za pomocą wniosku wprowadza się także bardziej precyzyjne przepisy dotyczące procesu zgłaszania incydentów, treści zgłoszeń i terminów, a także przewiduje się środki naprawcze i sankcje w celu zapewnienia egzekwowania przepisów.
- Państwa członkowskie będą miały 21 miesięcy od wejścia w życie dyrektywy na włączenie jej przepisów do swojego prawa krajowego.

Po postępach związanych z dyrektywą NIS 2 należy jak najszybciej zakończyć negocjacje dotyczące proponowanej **dyrektywy w sprawie odporności podmiotów krytycznych**[13] („dyrektywa CER"), która po przyjęciu i wdrożeniu powinna zwiększyć odporność podmiotów krytycznych na szereg zagrożeń, w tym ataki terrorystyczne, zagrożenia wewnętrzne lub sabotaż. Istotne jest również, aby poziom ambicji wyznaczony w dyrektywie w sprawie odporności podmiotów krytycznych odpowiadał poziomowi wyznaczonemu we wniosku Komisji oraz aby zachowana została spójność z kompromisem politycznym osiągniętym w kwestii dyrektywy NIS 2. Razem środki te zwiększą odporność i gotowość dzięki wprowadzeniu bardziej spójnego i solidnego systemu, w tym za pośrednictwem krajowych planów reagowania na incydenty i sytuacje kryzysowe. Były one również częścią wydanego w ubiegłym roku zalecenia Komisji[14] w sprawie utworzenia **wspólnej jednostki ds. cyberprzestrzeni**, w którym określono sposób współpracy na szczeblu operacyjnym poszczególnych podmiotów ekosystemu cyberbezpieczeństwa (dyplomatycznych, policyjnych, cywilnych i, w stosownych przypadkach, obronnych). Obecny krajobraz zagrożeń uwydatnia wartość takiej skutecznej współpracy między głównymi podmiotami.

Komisja w dalszym ciągu monitoruje wdrażanie unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci **5G**[15]. W tym kontekście 11 maja grupa współpracy NIS przyjęła sprawozdanie na temat bezpieczeństwa otwartej sieci dostępu radiowego[16]. Ponadto wciąż współpracuje ona z państwami członkowskimi w celu zapewnienia pełnej operacyjności Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa.

---

[13] COM(2020) 829.

[14] Zalecenie w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni |Kształtowanie cyfrowej przyszłości Europy (europa.eu)

[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

[16] Grupa współpracy NIS, *Report on the cybersecurity of Open RAN* [Sprawozdanie na temat bezpieczeństwa otwartej sieci dostępu radiowego], 11 maja 2022 r.

22 marca 2022 r. Komisja zaproponowała **nowe przepisy mające na celu ustanowienie wspólnych środków w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji we wszystkich instytucjach, organach i agencjach UE**. Przepisy te zwiększą odporność administracji UE i jej zdolność do reagowania na zagrożenia cyberbezpieczeństwa i cyberincydenty. Dzięki ujęciu tych działań we wspólne ramy zacieśniona zostanie współpraca międzyinstytucjonalna, a narażenie na ryzyko zostanie zminimalizowane. Za pośrednictwem proponowanego **rozporządzenia w sprawie cyberbezpieczeństwa w instytucjach, organach i agencjach UE**[17] wzmocniony zostanie mandat CERT-UE i powstanie nowa Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa, zwiększone zostaną zdolności w zakresie cyberbezpieczeństwa, a także propagowane będą regularne oceny dojrzałości i lepsza higiena cyberbezpieczeństwa. Na mocy proponowanego **rozporządzenia w sprawie bezpieczeństwa informacji**[18] ustanowiony zostanie minimalny zestaw przepisów i norm bezpieczeństwa informacji z myślą o zabezpieczeniu przetwarzania i wymiany informacji w przypadku wszystkich instytucji, organów i agencji UE, aby zapewnić lepszą i spójną ochronę przed zmieniającymi się zagrożeniami, na jakie narażone są ich informacje. Komisja wzywa Parlament Europejski i Radę do szybkiego przyjęcia tych środków.

Komisja zakończyła już konsultacje publiczne w sprawie środków służących zwiększeniu **cyberodporności** produktów cyfrowych i przygotowuje wniosek, który ma zostać opublikowany tej jesieni[19]. Wniosek ten będzie odnosił się do podatności na zagrożenia produktów cyfrowych i usług pomocniczych, które – chociaż stwarzają możliwości dla gospodarek i społeczeństw UE – powodują również nowe wyzwania, ponieważ im więcej urządzeń jest podłączonych do sieci, tym łatwiej o to, by cyberincydent miał wpływ na cały system, a tym samym zakłócił działalność gospodarczą i społeczną.

9 marca 2022 r. ministrowie UE odpowiedzialni za telekomunikację jednogłośnie przyjęli wezwanie z Nevers do wzmocnienia zdolności UE w zakresie cyberbezpieczeństwa, które obejmuje „wdrożenie nowego funduszu pomocy w sytuacjach kryzysowych związanych z cyberbezpieczeństwem, który ma zostać ustanowiony przez Komisję”[20]. Komisja zastanawia się nad najlepszym sposobem wykorzystania istniejących funduszy do wspierania działań zapobiegawczych i pomocowych.

Sektory krytyczne

Bezpieczeństwo dostaw **energii** do UE ma krytyczne znaczenie dla dobrostanu obywateli i sprawnego funkcjonowania naszych gospodarek, a obecna sytuacja uwydatniła konieczność wprowadzenia przejrzystych przepisów dotyczących cyberbezpieczeństwa w tym sektorze. Komisja pracuje nad kodeksem sieci dotyczącym cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej wymaganym na mocy rozporządzenia w sprawie energii elektrycznej[21], aby zapewnić zasady dotyczące ocen ryzyka, wspólnych wymogów

[17] COM(2022) 122.
[18] COM(2022) 119.
[19] Akt dotyczący cyberodporności – nowe przepisy dotyczące cyberbezpieczeństwa produktów cyfrowych i usług pomocniczych (europa.eu)
[20] 08.03.2022 r. – Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr)
[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 z dnia 5 czerwca 2019 r. w sprawie rynku wewnętrznego energii elektrycznej, Dz.U. L 158 z 14.6.2019, s. 54. Wniosek jest obecnie poddawany przeglądowi przez Agencję ds. Współpracy Organów Regulacji Energetyki.

minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego. Od czasu rosyjskiej agresji na Ukrainę cele kodeksu sieci dotyczącego cyberbezpieczeństwa są jeszcze bardziej istotne. Komisja rozpoczęła również współpracę strukturalną między ENISA, ENTSO-E[22], ENTSO gazu[23] i Wspólnotą Energetyczną w zakresie regularnego monitorowania sytuacji związanej z cyberbezpieczeństwem w sektorze energetycznym.

UE pracuje nad zapewnieniem bezpieczeństwa swoich partnerów, nie stwarzając dla siebie nowego ryzyka. Nadzwyczajna synchronizacja sieci elektroenergetycznych Ukrainy i Mołdawii z siecią Europy kontynentalnej nastąpiła w marcu 2022 r. po przyjęciu środków ograniczających ryzyko, w szczególności w odniesieniu do cyberbezpieczeństwa.

Wojna i sankcje spowodowały również wiele wyzwań związanych z unijnym **transportem**, począwszy od ryzyka dla bezpieczeństwa unijnego lotnictwa cywilnego i kierowców ciężarówek, którzy utknęli w strefach konfliktu, po zniszczenie ukraińskiej infrastruktury transportowej, odcięcie łańcuchów dostaw i zagrożenie dla światowego bezpieczeństwa żywnościowego. Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego, w ścisłej współpracy z Komisją i Eurocontrol – Europejską Organizacją ds. Bezpieczeństwa Żeglugi Powietrznej – od początku wojny zaleca operatorom, aby nie wykonywali lotów w przestrzeni powietrznej Ukrainy i unikali korzystania z przestrzeni powietrznej w promieniu 100 mil morskich od granicy białorusko- i rosyjsko-ukraińskiej.

Komisja pracuje również nad zwiększeniem gotowości i odporności unijnego sektora transportu. W szczególności w nowym planie awaryjnym dla transportu[24], przyjętym 23 maja, wykorzystano doświadczenia zdobyte zarówno w związku z pandemią COVID-19, jak i agresją wojskową Rosji wobec Ukrainy. W planie tym przewidziano zestaw 10 narzędzi, którymi UE i jej państwa członkowskie powinny się kierować przy wprowadzaniu nadzwyczajnych środków reagowania kryzysowego, w tym zapewnienie minimalnej jakości sieci połączeń, stworzenie odporności na zagrożenia cyberbezpieczeństwa i zagrożenia hybrydowe oraz zacieśnienie współpracy z partnerami międzynarodowymi w zakresie gotowości na wypadek sytuacji kryzysowej i reagowania kryzysowego. Podkreślono w nim również znaczenie regularnego testowania odporności na różne scenariusze kryzysowe wraz z odpowiednimi agencjami UE lub innymi podmiotami oraz w oparciu o istniejące procesy.

Zgodnie z ramami **bezpieczeństwa zdrowotnego w UE** wymiana informacji oparta na systemie wczesnego ostrzegania i reagowania, w tym wsparcie ewakuacji medycznej z Ukrainy, musi być chroniona przed cyberatakami, w związku z czym wzmacniane jest bezpieczeństwo systemu.

Współpraca z partnerami

UE nieustannie współpracuje ze swoimi partnerami międzynarodowymi, aby zapobiegać szkodliwym zachowaniom w cyberprzestrzeni, zniechęcać do nich, powstrzymywać przed nimi i reagować na nie. Rosyjska agresja na Ukrainę sprawiła, że współpraca w tej dziedzinie stała się ważniejsza niż kiedykolwiek. W związku z tym ESDZ pracuje nad wymianą wiedzy na temat orientacji sytuacyjnej i koordynacją reakcji na szkodliwe działania w cyberprzestrzeni wymierzone w Ukrainę, a także nad wsparciem dla Ukrainy i innych

[22] Europejska sieć operatorów systemów przesyłowych energii elektrycznej.
[23] Europejska sieć operatorów systemów przesyłowych gazu.
[24] COM(2022) 21.

państw w regionie, współpracując z partnerami, w tym USA i NATO, aby zapewnić komplementarność i uniknąć nakładania się działań.

Ścisła współpraca z USA pogłębiła się również w ramach Rady UE–USA ds. Handlu i Technologii. We wspólnym oświadczeniu[25] wydanym po majowym posiedzeniu ministerialnym w Paryżu podkreślono główną rolę Rady UE–USA ds. Handlu i Technologii w odnowionym partnerstwie transatlantyckim, które służy koordynacji wspólnych środków stosowanych przez UE i USA w obliczu rosyjskiej agresji na Ukrainę. Obie strony zgodziły się, że ścisła współpraca na rzecz zwiększenia odporności łańcuchów dostaw ma większe znaczenie niż kiedykolwiek wcześniej. Ponadto utworzono specjalną grupę zadaniową ds. publicznego finansowania bezpiecznej i odpornej infrastruktury cyfrowej w państwach trzecich, aby utorować drogę do wspólnego publicznego finansowania przez USA i UE projektów w zakresie technologii cyfrowych w państwach trzecich w oparciu o zbiór wspólnych, nadrzędnych zasad.

Strategiczny kompas przyjęty w marcu 2022 r. (zob. sekcja VII) przyczyni się do dalszego wzmocnienia unijnego zestawu narzędzi dla dyplomacji cyfrowej i pozwoli nadal pracować nad polityką UE w zakresie cyberobrony, by lepiej przygotować się na cyberataki i lepiej na nie reagować, w ramach szerszej strategii mającej na celu zwiększenie zdolności UE do działania w sytuacjach kryzysowych i obrony swoich interesów.

Wsparcie w zakresie cyberbezpieczeństwa dla Ukrainy i państw sąsiadujących

UE jeszcze przed wojną wspierała cyberodporność Ukrainy. Już w czerwcu 2021 r. UE i Ukraina przeprowadziły pierwszy dialog w sprawach cyberprzestrzeni i UE udzieliła wsparcia na rzecz cyberbezpieczeństwa i prężnej transformacji cyfrowej w ramach programu EU4Digital Ukraine o wartości 25 mln EUR. Inny program partnerski o wartości 1,5 mln EUR opracowano, aby pomóc ukraińskim instytucjom zajmującym się cyberbezpieczeństwem dostosować się do norm unijnych.

Po wybuchu wojny UE propaguje współpracę między unijnymi i ukraińskimi ekspertami ds. cyberbezpieczeństwa oraz koordynuje zapewnianie pomocy technicznej, sprzętu, oprogramowania i odpowiednich usług w celu zwiększenia cyberodporności i cyberobrony Ukrainy.

Ponadto UE pracuje nad oceną możliwości udzielenia średnioterminowego wsparcia dla Mołdawii, Gruzji i Bałkanów Zachodnich. Wspólna misja oceny potrzeb w zakresie cyberbezpieczeństwa w Mołdawii została przeprowadzona 3–4 marca 2022 r. i doprowadziła do przyjęcia specjalnego środka reagowania kryzysowego służącego szybkiemu zwiększeniu cyberbezpieczeństwa w tym państwie. Podobne wsparcie szybkiego reagowania przygotowywane jest dla szeregu wybranych państw Bałkanów Zachodnich uznawanych za szczególnie narażone na ryzyko w związku z ich dostosowaniem się do sankcji UE. Prowadzona jest również ocena ewentualnej dodatkowej pomocy dla Mołdawii w ramach Europejskiego Instrumentu na rzecz Pokoju.

III. PRZESTĘPCZOŚĆ ZORGANIZOWANA I TERRORYZM

[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108

Rosyjska agresja na Ukrainę zmusiła miliony osób do opuszczenia swoich domów, co znacznie zwiększyło ruch na granicach zewnętrznych UE. Do 18 maja niemal 6 mln osób przybyło do UE z Ukrainy i Mołdawii i jak dotąd 2,8 mln osób zarejestrowało się w celu uzyskania tymczasowej ochrony w UE. UE usiłowała zapewnić jak najszybsze i jak najbardziej elastyczne przyjęcie osób uciekających przed wojną, nie naruszając przy tym bezpieczeństwa na granicach zewnętrznych UE. UE zastosowała bezprecedensowe środki w celu zapewnienia osobom uciekającym przed wojną tymczasowej ochrony i zależy jej, aby wszystkie nowo przybyłe osoby były traktowane w sposób niedyskryminujący. Jednocześnie nie można lekceważyć potencjalnego ryzyka, które może wyniknąć przemieszczania się tak dużej liczby osób, i Unia, przy znacznym wsparciu odpowiednich agencji UE, pozostaje czujna na nowe zjawiska związane z przestępczością zorganizowaną i terroryzmem.

Silna strefa Schengen w obliczu zwiększonego zagrożenia

Zapewnienie wysokiego poziomu bezpieczeństwa w strefie **Schengen** i w UE nigdy nie było tak ważne jak w sytuacji podwyższonego zagrożenia wynikającego z wojny toczącej się tuż za granicą zewnętrzną UE.

Realizując ambitny program dotyczący strefy Schengen, określony w strategii z czerwca 2021 r., Komisja przyjęła w maju pierwsze sprawozdanie w sprawie stanu strefy Schengen[26]. Coroczny cykl Schengen jest nowym modelem zarządzania strefą Schengen, w ramach którego dokonuje się regularnych ocen jej stanu. Pomoże to w szybkim wykrywaniu niedociągnięć i zapewni skuteczne procedury działań następczych, tak aby strefa Schengen stała się silniejsza i bardziej odporna.

W tym pierwszym sprawozdaniu uznano konieczność zwiększenia starań na rzecz realizacji najważniejszych inicjatyw na szczeblu UE, w tym prowadzenia systematycznych kontroli wszystkich podróżnych na granicach zewnętrznych, przy pełnym wykorzystaniu mandatów Fronteksu i Europolu, a także proponowanych i dostępnych narzędzi transgranicznej współpracy policyjnej.

W szczególności nowa architektura unijnych systemów informacyjnych dotyczących granic, migracji i bezpieczeństwa oraz ich interoperacyjność stanowią podstawę starań na rzecz zwiększenia bezpieczeństwa wewnętrznego i usprawnienia zarządzania granicami. Zasadnicze znaczenie będzie miało skuteczne wdrożenie wszystkich elementów ram interoperacyjności zgodnie z ustalonymi terminami.

Czujność i koordynacja

Ściślejsza współpraca organów ścigania państw członkowskich i państw trzecich ma istotne znaczenie dla zapewnienia wiedzy na temat pojawiających się zagrożeń związanych z przestępczością i terroryzmem oraz podejmowania działań przeciwko siatkom przestępczym i osobom, które mogą próbować wykorzystać wojnę z Ukrainą. Państwa członkowskie i partnerzy operacyjni prowadzą aktywną wymianę istotnych i dostępnych informacji oraz danych wywiadowczych dotyczących przestępstw z Europolem, który przeprowadza kontrolę krzyżową i analizę tych informacji, a następnie przekształca je

[26] COM(2022) 301.

w użyteczne operacyjne powiadomienia wywiadowcze, takie jak powiadomienia wczesnego ostrzegania i oceny zagrożenia, które są udostępniane partnerom.

Przestępczość zorganizowana

Zorganizowane grupy przestępcze już znajdują sposoby na wykorzystanie obecnej sytuacji. Wstępna analiza danych wywiadowczych pozwoliła zidentyfikować schematy popełniania przestępstw w wielu obszarach, takich jak handel ludźmi, podrobione zgłoszenia przywozowe i wywozowe towarów, oszustwa internetowe, cyberprzestępczość i nielegalny handel bronią palną. Istnieją również dowody na to, że cyberprzestępcy, podając się za osoby zbierające fundusze dla Ukrainy, kradną pieniądze i kryptowaluty[27]. Z uwagi na obecną sytuację organizacje przestępcze z Ukrainy mogą próbować przenieść się w inne miejsce i kontynuować swoją działalność w UE.

Komisja i francuska prezydencja w Radzie UE pracowały wspólnie, a także z agencjami WSiSW UE, w szczególności z Europolem, nad uruchomieniem europejskiej multidyscyplinarnej platformy przeciwko zagrożeniom przestępstwami (**EMPACT**), aby oceniać i przewidywać istniejące lub pojawiające się zagrożenia poważną i zorganizowaną przestępczością oraz zapobiegać tym zagrożeniom i zwalczać je. 7 kwietnia 2022 r. Europol zorganizował posiedzenie EMPACT, w którym uczestniczyli przedstawiciele i eksperci z państw członkowskich UE i unijnej wspólnoty bezpieczeństwa i które poświęcone było zagrożeniom poważną i zorganizowaną przestępczością, które pojawiły się w wyniku wojny w Ukrainie. Omówiono na nim konkretne kroki, takie jak gromadzenie większej ilości danych wywiadowczych, realizacja nadzwyczajnych działań operacyjnych i przeformułowanie istniejących, a także dni wspólnych działań *ad hoc*.

CELBET (Zespół Ekspertów Celnych ds. Wschodniej i Południowo-Wschodniej Granicy Lądowej) – projekt współpracy finansowany przez Komisję Europejską – obserwuje rozwój sytuacji na granicy w ramach swojej misji zapewniania wsparcia operacyjnego i wytycznych dla funkcjonariuszy celnych oraz monitoruje zajęcia celne na przejściach granicznych na granicy UE (Polski, Słowacji, Węgier i Rumunii) z Ukrainą.

Działalność przestępcza i terrorystyczna

Chociaż jak dotąd w UE nie pojawiło się bezpośrednie zagrożenie terrorystyczne w związku z inwazją Rosji na Ukrainę, konieczność zachowania czujności jest oczywista.

Zwiększone ryzyko działalności przestępczej i terrorystycznej uwydatnia, jak istotne jest, by państwa członkowskie korzystały z odpowiednich baz danych UE, takich jak System Informacyjny Schengen, by w stosownych przypadkach wprowadzały do nich dane oraz by sprawdzały je podczas kontroli osób wjeżdżających do UE. Pomoże to zapewnić, aby osoby, które stanowią zagrożenie dla bezpieczeństwa wewnętrznego UE, były wykrywane na granicach zewnętrznych. Eu-LISA – Agencja Unii Europejskiej ds. Zarządzania

[27] Grupa Google'a ds. analizy zagrożeń odnotowała rosnącą liczbę podmiotów stwarzających zagrożenie, które wykorzystują wojnę w Ukrainie jako przynętę w kampaniach związanych z phishingiem i złośliwym oprogramowaniem. Analitycy z firmy Cyren, zajmującej się bezpieczeństwem internetowym, donoszą o wzroście liczby oszustw dotyczących kryptowalut, w których wykorzystuje się konflikt za pomocą fałszywych stron internetowych służących do przekazywania darowizn.

Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości – nieustannie dba o pełną dostępność i wydajność systemów zarządzania granicami UE. W wytycznych[28] dla państw członkowskich wyjaśniono, jak zrównoważyć konieczność zapewnienia sprawnej odprawy osób przybywających na granicę zewnętrzną przy jednoczesnym przeprowadzaniu niezbędnych kontroli bezpieczeństwa.

Gotowość

Oprócz zapewnienia wytycznych i koordynacji zwiększono gotowość UE poprzez oddelegowanie pracowników agencji UE.

Europol oddelegował zespoły operacyjne do państw członkowskich UE sąsiadujących z Ukrainą. Zespoły te składały się z zaproszonych funkcjonariuszy Europolu z państw członkowskich i ekspertów Europolu na Węgrzech, Litwie, w Polsce, Rumunii i na Słowacji oraz w Mołdawii[29]. Zaproszeni funkcjonariusze Europolu wspierają organy krajowe w przeprowadzaniu kontroli bezpieczeństwa drugiej linii na zewnętrznych granicach UE. Eksperci Europolu udzielają wsparcia polegającego na gromadzeniu i ocenie informacji w celu wykrywania zagrożeń terroryzmem i przestępczością, pomocy w prowadzeniu postępowań oraz identyfikacji osób stwarzających zagrożenie poprzez próby wjazdu do UE. Wspomniane zespoły operacyjne gromadzą informacje, które są wykorzystywane w ocenach zagrożenia przestępczością, udostępnianych państwom członkowskim. Takie czynności w zakresie gromadzenia danych wywiadowczych pozwalają Europolowi przewidywać rozwój sytuacji i koordynować działania operacyjne z państwami członkowskimi UE, aby reagować na działalność grup przestępczych próbujących wykorzystać wojnę w Ukrainie, oraz opierać się na aktywnej współpracy Europolu z ukraińskimi organami ścigania za pośrednictwem ukraińskiego urzędnika łącznikowego obecnego w głównej siedzibie Europolu w Niderlandach.

Europejska Agencja Straży Granicznej i Przybrzeżnej (**Frontex**) również jest obecna w państwach członkowskich i państwach sąsiadujących z UE, aby wspierać czynności związane z kontrolą graniczną: obecnie w całej UE, na Bałkanach Zachodnich i w Mołdawii znajduje się ponad 2 100 oddelegowanych funkcjonariuszy straży granicznej. **Europejski Urząd Wsparcia w dziedzinie Azylu (EASO)** oddelegował niemal 750 pracowników do południowych państw członkowskich UE i na Litwę, aby wesprzeć działania operacyjne, zwiększyć zdolności przyjmowania i pomóc przy procedurach azylowych.

Na podstawie obowiązującej **decyzji w sprawie konwencji z Prüm**[30], która zapewnia państwom członkowskim ramy do oddelegowania funkcjonariuszy organów ścigania do wspólnych operacji, takich jak wspólne patrole, Komisja i francuska prezydencja w Radzie Unii Europejskiej wystosowały wspólne pismo do wszystkich państw członkowskich, aby określić potrzeby i zwrócić się o oddelegowanie funkcjonariuszy policji w celu rozpoczęcia

[28] Komunikat Komisji zawierający wytyczne operacyjne dotyczące zarządzania granicami zewnętrznymi w celu ułatwienia przekraczania granicy między UE a Ukrainą, 2022/C 104 I/01.

[29] Na dzień 3 maja Europol oddelegował 1 pracownika Europolu i 3 zaproszonych funkcjonariuszy na Słowację, 1 funkcjonariusza Europolu do Polski, 1 funkcjonariusza Europolu i 4 zaproszonych funkcjonariuszy do Rumunii oraz 2 zaproszonych funkcjonariuszy na Węgry. 1 pracownik Europolu i 2 zaproszonych funkcjonariuszy zostało oddelegowanych do Mołdawii.

[30] Decyzje 2008/615/WSiSW 2008/616/WSiSW.

wspólnych patroli w państwach członkowskich UE pierwszej linii, na które masowe przekraczanie granicy w związku z wojną ma największy wpływ. Komisja będzie finansować te oddelegowania w ramach Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej.

Rozwiązanie problemu handlu ludźmi

Już od pierwszych dni wojny UE była czujna, jeśli chodzi o ryzyko związane z jednym konkretnym obszarem działalności przestępczej, który może skorzystać na ogromnych przepływach osób szukających bezpieczeństwa w UE. Istotne znaczenie ma uniemożliwianie działań handlarzom ludźmi, którzy obierają sobie za cel bezbronne osoby przemieszczające się, którymi są głównie **kobiety i dzieci**, wykorzystując na przykład fałszywe oferty transportu lub zakwaterowania.

W marcu Europol i Eurojust skierowały do odpowiednich organów krajowych powiadomienia wczesnego ostrzegania dotyczące potencjalnego handlu ludźmi i wykorzystywania ofiar przybywających z Ukrainy. Eurojust pomaga usprawnić wymianę informacji i przyspieszyć współpracę sądową, w tym z Ukrainą, a postępowania w sprawach handlu ludźmi zostały przekazane agencji w celu koordynacji.

Koordynator ds. zwalczania handlu ludźmi odbył posiedzenia z unijną siecią sprawozdawców krajowych i równoważnych struktur, agencjami wymiaru sprawiedliwości i spraw wewnętrznych oraz unijną platformą społeczeństwa obywatelskiego przeciwko handlowi ludźmi w celu wymiany informacji na temat działań niezbędnych do zapobiegania nadużyciom i ich zwalczania oraz ochrony ofiar. W kilku państwach członkowskich wszczęto postępowania dotyczące potencjalnych spraw.

UE szybko i sprawnie zapewniła skoordynowaną reakcję na to realne zagrożenie dla osób, które potrzebują jej pomocy. Państwom członkowskim wykonującym dyrektywę w sprawie tymczasowej ochrony szybko zapewniono wytyczne operacyjne[31], w tym dotyczące problemu handlu ludźmi, aby pomóc osobom uciekającym przed wojną w Ukrainie. W ramach 10-punktowego planu wzmocnienia europejskiej koordynacji przyjmowania osób uciekających przed wojną w Ukrainie[32], przedstawionego na posiedzeniu Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych 28 marca 2022 r., koordynator ds. zwalczania handlu ludźmi, we współpracy z agencjami UE i państwami członkowskimi, opracował wspólny plan zwalczania handlu ludźmi[33] dotyczący zapobiegania handlowi ludźmi i pomocy ofiarom. W szczególności skoncentrowano się na rejestrowaniu podmiotów i osób fizycznych (w tym wolontariuszy), które zamierzają zapewnić zakwaterowanie, transport i inne rodzaje pomocy, a także na sprawdzaniu przeszłości. Komisja nawiązała również współpracę z AUEA, aby pomóc w wykrywaniu ofiar handlu ludźmi podczas przeprowadzania kontroli stanu zdrowia w ośrodkach recepcyjnych. Małoletni bez opieki lub odseparowani od rodziców są szczególnie narażeni na znęcanie, wykorzystywanie seksualne lub przymusową przestępczość. Wspomniane wyżej wytyczne operacyjne zawierają także wskazówki mające pomóc państwom członkowskim w postępowaniu w przypadku przybycia dzieci,

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - PL - EUR-Lex (europa.eu).

[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en

a w szczególności małoletnich bez opieki, a także przyjmowania ich i udzielania im pomocy. Aby zwiększyć świadomość wśród osób zagrożonych, Komisja uruchomiła również specjalną stronę internetową z sekcją zawierającą praktyczne porady dotyczące sposobu unikania handlarzy ludźmi.

Niektóre działania mające na celu zwiększenie gotowości zostały podjęte konkretnie w odpowiedzi na nowe warunki wynikające z wojny, natomiast inne ważne środki wywodzą się z **inicjatyw ustawodawczych**, które były przygotowywane jeszcze przed rosyjską agresją na Ukrainę.

Komisja z zadowoleniem przyjmuje porozumienie osiągnięte w lutym 2022 r. w sprawie zmienionego mandatu[34] **Europolu,** który po wejściu w życie pozwoli Europolowi lepiej wspierać państwa członkowskie w zwalczaniu przestępczości zorganizowanej i terroryzmu. Agencja będzie wówczas dysponować odpowiednimi narzędziami i zabezpieczeniami, aby wspierać siły policyjne w analizowaniu dużych zbiorów danych na potrzeby prowadzenia postępowań w sprawie przestępstw oraz w opracowywaniu pionierskich metod walki z cyberprzestępczością. Zmiany te wiążą się ze wzmocnieniem ram ochrony danych, a także ze wzmocnionymi nadzorem parlamentarnym i rozliczalnością.

Pakiet dotyczący **współpracy policyjnej**, przedstawiony przez Komisję 8 grudnia 2021 r.[35] i obecnie będący przedmiotem negocjacji, wzmocni współpracę między funkcjonariuszami organów ścigania w państwach członkowskich dzięki szybszej, łatwiejszej i bezpieczniejszej wymianie danych, a także dzięki zacieśnieniu operacyjnej współpracy policyjnej w terenie i zwiększeniu jej skuteczności. Komisja wzywa Parlament Europejski i Radę do szybkiego przyjęcia tego pakietu.

Po ich przyjęciu i wdrożeniu wspomniane wnioski ustawodawcze przyczynią się do zapewnienia wsparcia organom ścigania w zwalczaniu transgranicznej przestępczości zorganizowanej. Będzie to szczególnie istotne w sytuacjach, w których organizacje przestępcze z Ukrainy mogą próbować przenieść się w inne miejsce i kontynuować swoją działalność w UE.

Misja doradcza UE w Ukrainie wspiera reformę organów ścigania i praworządności w tym kraju od 2014 r. W marcu 2022 r. zmieniono mandat misji, co umożliwiło udzielanie wsparcia na przejściach granicznych Ukrainy z Polską, Rumunią i Słowacją i przyczyniło się do zwiększenia orientacji sytuacyjnej w zakresie transgranicznej działalności przestępczej, w tym handlu ludźmi, oraz przepływu towarów do Ukrainy w ramach pomocy humanitarnej.

IV. BROŃ, MATERIAŁY NIEBEZPIECZNE I INCYDENTY KRYTYCZNE

Wojna znacznie zwiększyła obrót bronią palną i innymi rodzajami broni w samej Ukrainie, co stwarza nowe zagrożenia dla UE i innych państw sąsiadujących z Ukrainą.

Czujność i koordynacja

[34] COM(2020) 796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.

W wydanych w marcu wytycznych operacyjnych przedstawiono porady dla państw członkowskich dotyczące sposobów sprostania wyzwaniu, jakim jest zwiększony obrót bronią palną w okresie masowego napływu osób na granicę zewnętrzną UE[36]. W wytycznych tych podkreślono, że należy stale kontrolować obecność broni palnej i że nie można dopuścić do sytuacji, w której osoba bez zezwolenia wjechałaby do UE z bronią palną. Jeżeli organy ukraińskie zgłoszą brak którejkolwiek z tych sztuk broni palnej, państwa członkowskie powinny zarejestrować je w Systemie Informacyjnym Schengen.

Niezwykle istotne jest, aby wszystkie dostawy broni palnej do Ukrainy były odpowiednio rejestrowane, z podaniem wszystkich istotnych informacji (w tym typu, kraju i roku produkcji, marki, modelu, kalibru, numeru seryjnego) w celu ułatwienia identyfikowalności tej broni palnej zarówno w Ukrainie, jak i w UE.

UE publicznie potępiła lekkomyślne wojskowe ataki Rosji na cywilne obiekty jądrowe, biologiczne i chemiczne w Ukrainie i w bezpośrednim sąsiedztwie tych obiektów, a także wszelkie działania zagrażające bezpieczeństwu tych obiektów. Komisja monitoruje sytuację w Ukrainie, szczególną uwagę zwracając na zagrożenie radiologiczne, które budzi największe obawy z punktu widzenia bezpieczeństwa wewnętrznego UE[37]. Komisja monitoruje również potencjalne zagrożenia chemiczne i ustanowiła wewnętrzny mechanizm koordynacji na wypadek gdyby konieczne było szybkie przeprowadzenie oceny ryzyka.

Gotowość

Ukraina jest już jednym z państw, które w Planie działania UE w sprawie nielegalnego handlu bronią palną na lata 2020–2025 uznano za kluczowe dla podjęcia konkretnych działań na szczeblu zewnętrznym. Prowadzone jest także specjalne działanie operacyjne w regionie obejmującym Ukrainę w ramach komponentu EMPACT dotyczącego broni palnej. Biorąc jednak pod uwagę ryzyko przekierowania broni palnej, niezbędne będzie zrealizowanie konkretnych projektów finansowanych przez UE, a także współpraca operacyjna z Europolem, Fronteksem i komponentem EMPACT dotyczącym broni palnej. Komisja przedstawi wkrótce wniosek dotyczący zmiany rozporządzenia w sprawie broni palnej[38] odnoszącej się do wywozu, przywozu i tranzytu broni palnej do użytku cywilnego, jako część ogólnych ram prawnych i operacyjnych mających na celu zapobieganie handlowi bronią palną, wykrywanie go, prowadzenie postępowań przygotowawczych w jego sprawie i ściganie go.

Aby zwiększyć gotowość i zdolność reagowania UE na zagrożenia dla zdrowia publicznego, takie jak zagrożenia CBRJ, Komisja tworzy strategiczne rezerwy zdolności reagowania poprzez Unijny Mechanizm Ochrony Ludności finansowany przez Urząd ds. Gotowości i Reagowania na Stany Zagrożenia Zdrowia (HERA)[39]. Służby Komisji współpracują nad

---

[36] Komunikat Komisji zawierający wytyczne operacyjne dotyczące zarządzania granicami zewnętrznymi w celu ułatwienia przekraczania granicy między UE a Ukrainą, 2022/C 104 I/01.

[37] Komisja zorganizuje – we współpracy z partnerami z USA – warsztaty poświęcone zagrożeniom związanym z materiałami radiologicznymi znajdującymi się w szpitalach, nad którymi traci się kontrolę regulacyjną.

[38] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 258/2012 z dnia 14 marca 2012 r. wdrażające art. 10 Protokołu Narodów Zjednoczonych przeciwko nielegalnemu wytwarzaniu i obrotowi bronią palną, jej częściami i komponentami oraz amunicją, uzupełniającego Konwencję Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej (protokół NZ w sprawie broni palnej), oraz ustanawiające zezwolenia na wywóz i środki dotyczące przywozu i tranzytu dla broni palnej, jej części i komponentów oraz amunicji.

[39] Plan prac HERA na 2022 r. (europa.eu)

stworzeniem strategicznych zapasów rescEU wynoszących 540,5 mln EUR. Zapasy te będą obejmować sprzęt, leki, szczepionki i inne środki terapeutyczne stosowane w leczeniu pacjentów narażonych na działanie czynników nadzwyczajnych związanych z CBRJ, jak również rezerwę rescEU na potrzeby dekontaminacji, w skład której wchodzi sprzęt do dekontaminacji oraz zespoły ekspertów ds. reagowania. W pierwszej kolejności UE bezzwłocznie uruchomiła swoją rezerwę medyczną rescEU, aby zakupić tabletki jodku potasu, które można wykorzystać do ochrony ludzi przed szkodliwymi skutkami promieniowania, a także w inne artykuły pilnie potrzebne w Ukrainie. Dotychczas za pośrednictwem Unijnego Mechanizmu Ochrony Ludności, z pomocą Francji i Hiszpanii, do Ukrainy dostarczono już niemal 3 mln tabletek jodku.

V. SKOORDYNOWANE DZIAŁANIA MAJĄCE NA CELU POCIĄGNIĘCIE DO ODPOWIEDZIALNOŚCI ZA ROSYJSKĄ AGRESJĘ

UE odgrywa zasadniczą rolę w działaniach społeczności międzynarodowej mających na celu wywarcie presji na Rosję, by zaprzestała niedopuszczalnej i sprzecznej z prawem międzynarodowym agresji przeciwko państwu ukraińskiemu i cywilom uwikłanym w konflikt. Presja ta obejmuje środki służące wyciągnięciu konsekwencji wobec sprawców, w tym dotkliwe sankcje, oraz działania umożliwiające wykrycie i ułatwienie ścigania zbrodni wojennych.

Środki ograniczające i konfiskata

Po uznaniu przez Rosję 21 lutego 2022 r. niekontrolowanych przez rząd obszarów w obwodzie donieckim i ługańskim w Ukrainie oraz inwazji na Ukrainę 24 lutego 2022 r. UE nałożyła największą w historii serię środków ograniczających na Rosję. Dotychczas przyjęto pięć pakietów sankcji. Środki te koncentrują się na najważniejszych sektorach, w tym na sektorze finansów, handlu, transportu, obrony i mediów, i są wymierzone w elity polityczne i wojskowe, a także znaczących rosyjskich i białoruskich oligarchów. Na liście znajduje się już ponad 1 000 osób fizycznych i 80 podmiotów. W Radzie toczą się dyskusje nad szóstym pakietem sankcji.

Wpływ tych i wcześniejszych środków ograniczających przeciwko osobom fizycznym i przedsiębiorstwom rosyjskim i białoruskim będzie tak silny, jak silne będzie ich egzekwowanie. Koordynacja UE może w znacznym stopniu przyczynić się do zniwelowania potencjalnych luk, a Komisja udziela zainteresowanym stronom wszechstronnego wsparcia w postaci pisemnych wytycznych, spotkań zainteresowanych stron i specjalnej grupy ekspertów oraz szeregu zasobów ułatwiających zachowanie zgodności.

Ponadto Komisja utworzyła grupę zadaniową „Freeze and Seize", do której należą służby Komisji, państwa członkowskie, Eurojust i Europol. Jak dotąd państwa członkowskie zgłosiły, że zamroziły aktywa o wartości 9,89 mld EUR[40]. 11 kwietnia Europol, wspólnie z państwami członkowskimi, Eurojustem i Fronteksem, rozpoczął operację „Oscar" mającą na celu wsparcie prowadzenia dochodzeń finansowych i postępowań przygotowawczych dotyczących mienia pochodzącego z przestępstwa należącego do osób fizycznych i prawnych objętych sankcjami UE w związku z wojną Rosji przeciwko Ukrainie. Unijna grupa zadaniowa „Freeze and Seize" ściśle współpracuje z Grupą Zadaniową ds. Rosyjskich Elit, Pełnomocników i Oligarchów (grupą zadaniową REPO), utworzoną przez państwa grupy G7

[40] Zablokowano również aktywa rosyjskiego banku centralnego w kwocie około 23 mld EUR.

(Kanadę, Francję, Niemcy, Włochy, Japonię, Zjednoczone Królestwo, Stany Zjednoczone) oraz partnerów o podobnych poglądach, takich jak Australia, a także z grupą zadaniową KleptoCapture z USA i z ukraińską grupą zadaniową.

Grupa zadaniowa „Freeze and Seize" służy jako platforma koordynująca i ułatwiająca wymianę informacji i doświadczeń między państwami członkowskimi oraz dostarczająca wytycznych dotyczących wdrażania sankcji, a także usprawniająca wymianę najlepszych praktyk w zakresie postępowań przygotowawczych i konfiskaty. W szczególności istotne jest, aby organy ścigania były czujne i aktywne w odniesieniu do potencjalnych przestępstw popełnianych przez osoby fizyczne i podmioty objęte sankcjami. Grupa zadaniowa ma również na celu przyspieszenie dyskusji na temat możliwości wykorzystania skonfiskowanych środków, na przykład jako wkładu w odbudowę Ukrainy.

Obecnie Komisja przyjmuje pakiet dotyczący **odzyskiwania i konfiskaty mienia**[41], w którym uwzględniono doświadczenia zdobyte podczas wdrażania unijnych środków ograniczających wobec osób fizycznych i podmiotów z Rosji i Białorusi. Ułatwi on skuteczne wdrażanie unijnych środków ograniczających w całej Unii, umożliwiając szybkie wykrywanie i identyfikowanie mienia będącego własnością osób lub podmiotów objętych takimi środkami lub kontrolowanego przez te osoby lub podmioty. Wzmocnione ramy odzyskiwania i konfiskaty mienia będą miały zastosowanie również do naruszenia środków ograniczających, a tym samym zapewnią skuteczne wykrywanie i zamrażanie korzyści pozyskanych w wyniku naruszenia środków ograniczających, zarządzanie tymi dochodami i ich konfiskatę. W celu zapewnienia, aby mienie osób fizycznych i podmiotów naruszających środki ograniczające mogło być rzeczywiście konfiskowane, Komisja przyjmuje obecnie także wnioski dotyczące decyzji Rady w sprawie dodania naruszeń sankcji do wykazu przestępstw w UE określonych w art. 83 ust. 1 TFUE[42] wraz z komunikatem[43], z myślą o przedstawieniu wniosku dotyczącego dyrektywy w sprawie zbliżenia definicji przestępstw i kar za naruszenie środków ograniczających.

W bardziej ogólnym ujęciu pakiet ten stanowi istotny etap w zwalczaniu przestępczości zorganizowanej. Jest on zgodny ze zobowiązaniami Komisji podjętymi w strategii w zakresie unii bezpieczeństwa oraz strategii zwalczania przestępczości zorganizowanej 2020-2025[44]. W jego ramach zmienia się dyrektywę w sprawie konfiskaty z 2014 r., decyzję Rady z 2007 r. w sprawie biur ds. odzyskiwania mienia oraz decyzję ramową z 2005 r. w sprawie konfiskaty korzyści, narzędzi i mienia pochodzących z przestępstwa w celu wzmocnienia zdolności w zakresie wykrywania i identyfikacji, a ostatecznie konfiskaty nielegalnych zysków, co jest odpowiedzią na bardzo niskie wskaźniki konfiskaty w UE[45]. Dzięki pakietowi rozszerzono zakres uwzględnionych przestępstw oraz przepisy dotyczące konfiskaty, w przypadkach gdy wydanie wyroku skazującego za konkretne przestępstwo jest niemożliwe, ale mienie wyraźnie pochodzi z działalności przestępczej. Dzięki tej zmianie wzmocnione zostanie również skuteczne zarządzanie zamrożonym i skonfiskowanym mieniem oraz zwiększone zostaną zdolności biur ds. odzyskiwania mienia do wykrywania i identyfikowania nielegalnego mienia. Nowe unijne ramy odzyskiwania mienia zostały

[41] COM(2022) 245.
[42] COM(2022) 247.
[43] COM(2022) 249.
[44] COM(2021) 170.
[45] Europol szacuje, że jedynie 2 % mienia pochodzącego z przestępstwa jest zamrożone (2,4 mld EUR), a 1 % skonfiskowane (1,2 mld EUR), natomiast dochody z działalności przestępczej na głównych rynkach przestępczych w UE w 2019 r. wyniosły 139 mld EUR (1 % produktu krajowego brutto Unii).

opracowane z myślą o złożonych sposobach działania organizacji przestępczych, które często działają w wymiarze transgranicznym i stosują różne metody ukrywania swojego mienia, w tym za pomocą kryptoaktywów.

Skoordynowana reakcja wymiaru sprawiedliwości

Na szczeblu UE prowadzone są również prace nad zapewnieniem skoordynowanej reakcji wymiaru sprawiedliwości na zarzuty popełnienia **zbrodni międzynarodowych** w Ukrainie, tak by możliwe było pociągnięcie sprawców do odpowiedzialności.

Dwa państwa członkowskie i Ukraina powołały wspólny zespół dochodzeniowo-śledczy (JIT) w celu przeprowadzenia postępowań przygotowawczych w sprawie zbrodni wojennych, zbrodni przeciwko ludzkości i innych zarzutów popełnienia zbrodni międzynarodowych na terytorium Ukrainy. Eurojust udziela temu zespołowi dochodzeniowo-śledczemu wsparcia prawnego, analitycznego, finansowego i logistycznego. 25 kwietnia 2022 r. Urząd Prokuratora Międzynarodowego Trybunału Karnego dołączył do zespołu dochodzeniowo-śledczego jako uczestnik[46] i oczekuje się, że wkrótce dołączą kolejni uczestnicy.

25 kwietnia 2022 r. Komisja przedstawiła wniosek dotyczący zmiany rozporządzenia w sprawie Eurojustu[47], tak aby Eurojust mógł zabezpieczać, analizować i przechowywać dowody związane z najpoważniejszymi zbrodniami wagi międzynarodowej. Eurojust i Europol będą nieustannie ściśle współpracować przez cały czas realizacji tego procesu. Zasadniczą rolę w koordynowaniu reakcji wymiaru sprawiedliwości odgrywa również sieć punktów kontaktowych ds. ścigania ludobójstwa, której sekretariat prowadzi Eurojust i która przygotowała atlas organizacji pozarządowych działających obecnie w Ukrainie, a także wspiera praktyków krajowych z państw członkowskich i Ukrainy prowadzących bieżące sprawy związane z wojną.

W kwietniu 2022 r. Rada dodatkowo zmieniła mandat **misji doradczej UE w Ukrainie**, co umożliwiło udzielenie przez misję wsparcia organom ukraińskim w prowadzeniu dochodzeń w sprawie wszelkich zbrodni międzynarodowych popełnionych w kontekście rosyjskiej agresji wojskowej oraz w ich ściganiu. Misja zapewni organom ukraińskim doradztwo strategiczne dotyczące prowadzenia dochodzeń i ścigania zbrodni międzynarodowych, niezbędnych zmian w ustawodawstwie ukraińskim, strategii komunikacji, jak również szkolenia z zakresu powiązanych kwestii. Misja uczestniczy w wielu inicjatywach na rzecz koordynacji w tym kontekście oraz, wspólnie z delegaturą Unii, wchodzi w skład grupy doradczej USA-UE ds. masowych aktów okrucieństwa w Ukrainie.

VI. ZAGRANICZNA MANIPULACJA INFORMACJAMI I INGERENCJA W INFORMACJE

Aktualne wydarzenia geopolityczne uwypukliły ryzyko ingerencji zagranicznej. Agresji wojskowej Rosji wobec Ukrainy towarzyszą działania związane z zagraniczną **manipulacją informacjami i ingerencją w informacje**. Bezpodstawne oskarżenia o „nazizm” i „ludobójstwo” wobec rządu ukraińskiego, działania pod obcą banderą i nieuzasadnione zarzuty wobec NATO i Zachodu są wykorzystywane do usprawiedliwienia brutalnych ataków na Ukrainę, natomiast wolność słowa i niezależne doniesienia w Rosji są tłumione.

[46] https://www.eurojust.europa.eu/eurojust-and-the- war-in-ukraine
[47] COM(2022) 187 final.

Nieustannie istnieje ryzyko manipulacji materiałami audiowizualnymi i dezinformacji, które Rosja może próbować wykorzystać jako pretekst do kolejnych ataków wojskowych, do osłabienia zdecydowanego ukraińskiego oporu, do podzielenia społeczności międzynarodowej w jej sprzeciwie wobec wojny lub do zasiania wątpliwości co do naruszania przez Rosję prawa międzynarodowego. W Strategicznym kompasie UE zobowiązała się do zdecydowanego reagowania na zagraniczne manipulacje informacjami i ingerencje w informacje oraz do zwiększenia swojej odporności i zdolności w zakresie przeciwdziałania takim zagrożeniom[48]. Manipulowanie demokratyczną debatą w UE jest przedmiotem europejskiego planu działania na rzecz demokracji, czyli skoordynowanego planu Komisji mającego na celu przeciwdziałanie dezinformacji i wzmocnienie odporności demokratycznej[49].

Czujność i koordynacja

Unia Europejska zareagowała zdecydowanymi i skoordynowanymi działaniami na rosyjską kampanię dezinformacyjną prowadzoną w kontekście agresji wojskowej wobec Ukrainy. UE ściśle współpracuje z państwami członkowskimi za pośrednictwem systemu wczesnego ostrzegania oraz z partnerami międzynarodowymi, takimi jak NATO, USA, Kanada i mechanizm szybkiego reagowania grupy G7, aby wymieniać się spostrzeżeniami na temat tendencji i taktyk manipulacji stosowanych przez Kreml. Prace nad ujawnieniem manipulacji Kremla zostały zintensyfikowane, w szczególności za pomocą strony internetowej EUvsDisinfo, na której publikowane są informacje w języku angielskim, rosyjskim, ukraińskim i innych językach, z myślą o przekazywaniu faktycznych informacji w UE, Ukrainie i regionie, a także w Rosji. Od 2 marca transmisja i nadawanie przez kanały rosyjskich mediów państwowych RT i Sputnik w UE lub skierowane do UE są zawieszone w wyniku przyjęcia przez UE środków ograniczających. Sygnatariusze kodeksu postępowania w zakresie zwalczania dezinformacji[50] – platformy internetowe, wiodące sieci społecznościowe, reklamodawcy i przedstawiciele branży reklamowej – podejmują pilne działania w celu ograniczenia dezinformacji związanej z rosyjską agresją wobec Ukrainy. Komisja i ESDZ monitorują te starania. Z przekazanych informacji wynika, że platformy wzmocniły swoje narzędzia monitorowania i interwencji związane z wojną.

Ponadto szybko podejmowane są działania mające na celu wsparcie państw Azji Środkowej i Bałkanów Zachodnich w zwiększaniu odporności informacyjnej i przeciwdziałaniu zagranicznym manipulacjom informacjami i dezinformacji.

Gotowość

Jawne stosowanie zagranicznych manipulacji informacjami i ingerencji w informacje, w tym dezinformacji, jako jednego z narzędzi zagrożeń hybrydowych, sprawiło, że działania następcze w związku z europejskim planem działania na rzecz demokracji stały się jeszcze pilniejszą kwestią. W ostatnich miesiącach instytucje Unii wspierały państwa członkowskie w zwalczaniu zagranicznych manipulacji informacjami i ingerencji w informacje, w szczególności w ramach systemu szybkiego ostrzegania, udostępniając im swoje spostrzeżenia na temat taktyk wykorzystywanych przez podmioty stosujące takie manipulacje i ingerencje oraz na temat strategii reagowania. Prowadzone są dyskusje nad dalszym

[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pl/pdf
[49] COM(2020) 790.
[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

wzmocnieniem ogólnego reagowania UE na zagraniczne manipulacje informacjami i ingerencje w informacje na podstawie dokumentu koncepcyjnego przedstawionego przez ESDZ, dotyczącego opracowania specjalnego **zestawu narzędzi** do walki z tym zagrożeniem. Dzięki temu połączone zostaną istniejące środki wewnętrzne i nowe narzędzia UE w ramach wspólnej polityki zagranicznej i bezpieczeństwa. Przyczynią się do tego również zintensyfikowane działania grupy zadaniowej Stratcom powołanej w ramach Europejskiej Służby Działań Zewnętrznych[51] oraz Komisji.

Po wybuchu wojny w Ukrainie Europejskie Obserwatorium Mediów Cyfrowych powołało grupę zadaniową ds. dezinformacji i koordynuje działania weryfikatorów informacji i naukowców w swojej sieci. Obserwatorium to przeprowadziło analizę dotyczącą tego, jak szybko zwolennicy teorii spiskowych na temat COVID-19 zaczęli rozpowszechniać prorosyjskie fałszywe informacje, co zaobserwowano w wielu państwach członkowskich[52].

Wniosek dotyczący aktu o usługach cyfrowych ma na celu dostosowanie do szybko rozwijających się technologii cyfrowych oraz określenie, co to oznacza w odniesieniu do wyzwań technologicznych i demokratycznych, takich jak mowa nienawiści, dezinformacje w internecie i strategie destabilizacji. Znaczne postępy w negocjacjach prowadzonych przez Parlament Europejski i Radę powinny umożliwić szybkie przyjęcie pakietu.

VII. SZERSZA GOTOWOŚĆ

W czasie, gdy w Europie znów toczy się wojna, a także gdy zachodzą poważne zmiany geopolityczne, koordynacja w zakresie bezpieczeństwa w UE została zwiększona przy wykorzystaniu inicjatyw, które były przygotowywane jeszcze przed rosyjską agresją na Ukrainę. Inicjatywy dotyczące przede wszystkim bezpieczeństwa zewnętrznego UE mają znaczący wpływ na wewnętrzną agendę unii bezpieczeństwa.

15 lutego 2022 r. Komisja przedstawiła **pakiet dotyczący obronności**[53] zawierający szereg inicjatyw w obszarach o zasadniczym znaczeniu dla obronności i bezpieczeństwa w UE. Ten wkład Komisji w obronność i bezpieczeństwo w Europie obejmuje pełen zakres wyzwań. Zaproponowano w nim konkretne działania na rzecz bardziej zintegrowanego i konkurencyjnego europejskiego rynku obronnego, w szczególności poprzez zacieśnienie współpracy w ramach UE i osiągnięcie korzyści skali. Obejmuje on również Plan działania w zakresie technologii krytycznych dla bezpieczeństwa i obronności mający na celu pobudzenie badań naukowych, rozwoju technologicznego i innowacji w tych sektorach oraz zmniejszenie zależności w zakresie technologii krytycznych i łańcuchów wartości. Pakiet ma na celu także wzmocnienie wymiaru obronnego przestrzeni kosmicznej na szczeblu UE Ponadto przeanalizowano w nim sposób, w jaki Komisja mogłaby zintensyfikować działania na rzecz zwalczania zagrożeń hybrydowych, w tym w dziedzinie cyberbezpieczeństwa,

[51] Dział ds. komunikacji strategicznej, grup zadaniowych i analizy informacji Europejskiej Służby Działań Zewnętrznych udziela wsparcia w zakresie komunikacji strategicznej przy realizacji polityki zagranicznej i bezpieczeństwa UE w powiązanych regionach priorytetowych (południowe i wschodnie sąsiedztwo, Bałkany Zachodnie) poprzez opracowywanie i wdrażanie konkretnych działań z zakresu komunikacji strategicznej ukierunkowanych na propagowanie polityki, wartości, celów i interesów UE.

[52] https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/

[53] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en

zwiększyć mobilność wojskową w Europie i poza nią oraz w dalszym ciągu dążyć do sprostania wyzwaniom dotyczącym zmiany klimatu związanym z obronnością. W celu uzupełnienia tych prac, we wspólnym komunikacie **„Analiza luk inwestycyjnych w zakresie obronności i dalsze działania”**[54] z 18 maja rozważono luki w zdolnościach i przemyśle, które należy wyeliminować, aby wesprzeć najbardziej narażone państwa członkowskie UE i określić środki łagodzące stwierdzone braki.

Odporność UE na te zagrożenia wymaga również przyjęcia podejść opartych na zdolnościach we wszystkich sektorach bezpieczeństwa, które zaleca się w planie działania Komisji na rzecz synergii między przemysłem cywilnym, obronnym i kosmicznym[55]. Trwają prace nad upowszechnianiem podejść opartych na zdolnościach w dziedzinie bezpieczeństwa wewnętrznego i egzekwowania prawa.

21 marca 2022 r. Rada przyjęła **Strategiczny kompas na rzecz bezpieczeństwa i obrony**[56], który wkrótce potem został zatwierdzony przez Radę Europejską. W Kompasie przedstawiono ambitny plan działania na rzecz wzmocnienia polityki bezpieczeństwa i obrony UE do 2030 r. Ma on na celu uczynienie z UE silniejszego i dysponującego większymi zdolnościami gwaranta bezpieczeństwa, który chroni swoich obywateli i przyczynia się do międzynarodowego pokoju i bezpieczeństwa. Określono w nim konkretne propozycje, wraz z bardzo dokładnym harmonogramem ich realizacji, z myślą o zwiększeniu zdolności UE do zdecydowanego działania w przypadku kryzysów.

Jednym z osiągnięć w ramach Strategicznego kompasu jest opracowanie **unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym**, który powinien zapewnić ramy skoordynowanej reakcji na kampanie hybrydowe mające wpływ na UE i jej państwa członkowskie, w tym środków wewnętrznych i zewnętrznych. Po określeniu wyjściowych poziomów odporności sektorowej, którego dokonano na początku 2022 r.[57], zostanie zakończona analiza luk i potrzeb. To właśnie w tych ramach UE będzie nadal budować gotowość, odporność i zdolność reagowania na zagrożenia wynikające z agresji Rosji i wszelkich innych prób destabilizowania demokracji i wielostronnego porządku opartego na zasadach.

VIII. PERSPEKTYWY

W przyszłości UE będzie musiała zachować szczególną czujność wobec zmieniających się zagrożeń oraz budować **gotowość i odporność na wszelkie możliwości**. Skutki wojny mogą przybrać różne formy, z których nie wszystkie można już ocenić.

Nie wiadomo jeszcze, w jakim stopniu ukraińskie siatki przestępcze przesiedliły się. Sprawy prowadzone dotychczas przez Eurojust wskazują na tendencję w zakresie przemytu heroiny z Afganistanu do UE przez Ukrainę, co zostało potwierdzone przez Europejskie Centrum

[54] JOIN(2022) 24.
[55] COM(2021) 70.
[56] Strategiczny kompas na rzecz bezpieczeństwa i obrony – dla Unii Europejskiej, która chroni swoich obywateli, swoje wartości i interesy oraz przyczynia się do międzynarodowego pokoju i bezpieczeństwa: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pl/pdf
[57] SWD(2022) 21 final.

Monitorowania Narkotyków i Narkomanii (EMCDDA)[58]. Niestabilna sytuacja może utrudnić działania na rzecz zwalczania handlu heroiną prowadzonego tą drogą, co stwarza ryzyko potencjalnego wzrostu napływu narkotyków do UE.

W przypadku niektórych zagrożeń dla UE istnieje większe prawdopodobieństwo ich nasilenia się po zakończeniu walk lub w czasie potencjalnych przerw w ich prowadzeniu. Szczególna uwaga zostanie zwrócona na obrót bronią palną, przy czym ryzyko to wzrośnie po ustaniu walk w Ukrainie. Doświadczenia z przeszłości wskazują również na ryzyko, że powrót zagranicznych bojowników, którzy zdobyli doświadczenie bojowe i mogli mieć kontakt z grupami ekstremistycznymi, może w późniejszym czasie doprowadzić do działań terrorystycznych w UE. To potencjalne zjawisko należy uważnie monitorować, a Komisja już teraz ułatwia dyskusje między państwami członkowskimi na temat wyzwań wynikających z powrotu zagranicznych ochotników z przeszłością związaną z brutalnym ekstremizmem.

W świetle tych potencjalnych zagrożeń istotne jest, aby w dalszym ciągu realizować strategię w zakresie unii bezpieczeństwa, w tym wdrażać kluczowe strategie, takie jak strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, strategia zwalczania przestępczości zorganizowanej (2020–2025), plan dla UE w dziedzinie zwalczania terroryzmu (2020–2025), plan działania UE w sprawie nielegalnego handlu bronią palną (2020–2025), strategia UE w zakresie zwalczania handlu ludźmi (2021–2025), strategia UE w dziedzinie narkotyków (2021–2025).

Wciąż będą prowadzone starania, aby zapewnić UE niezbędne ramy legislacyjne. Na przykład Komisja przygotowuje ocenę skutków w odniesieniu do wniosku dotyczącego regulacji wprowadzania do obrotu i stosowania chemikaliów wysokiego ryzyka.

IX. WNIOSKI

Unia bezpieczeństwa nadal spełnia swoją rolę w przygotowaniu UE i jej państw członkowskich do zwalczania istniejących i potencjalnych zagrożeń. Rosyjska agresja na Ukrainę pokazała, jak szybko teoretyczne zagrożenia mogą stać się realne, i uwypukliła znaczenie czujności, koordynacji i gotowości.

Niniejsze czwarte sprawozdanie z postępu prac w realizacji strategii w zakresie unii bezpieczeństwa wskazuje, że UE jest w stanie się dostosować, nawet w obliczu wyjątkowych i nieoczekiwanych zagrożeń, takich jak rosyjska agresja na Ukrainę. Zdecydowana realizacja strategii w zakresie unii bezpieczeństwa jest ważniejsza niż kiedykolwiek.

[58] *Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data)* [Sprawozdanie na temat sytuacji związanej z narkotykami i alkoholem w Ukrainie za 2020 r. (według danych z 2019 r.)], OEDT, *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery* [Powstrzymanie przemytu substytutu heroiny we Francji, w Polsce i Ukrainie, w tym planowanie i przeprowadzenie kontrolowanej dostawy], 2021/00446, Eurojust, maj 2020 r.