Rada
Unii Europejskiej

Bruksela, 18 października 2023 r.
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	18 października 2023 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2023) 665 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY w sprawie szóstego sprawozdania z postępu prac w realizacji strategii UE w zakresie unii bezpieczeństwa

Delegacje otrzymują w załączeniu dokument COM(2023) 665 final.

Zał.: COM(2023) 665 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 18.10.2023 r.
COM(2023) 665 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

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

I. Wprowadzenie

Trzy lata temu Komisja przyjęła strategię w zakresie unii bezpieczeństwa na lata 2020–2025[1], w której określono główne priorytety Unii w dziedzinie bezpieczeństwa. Od tego czasu udało się poczynić znaczne postępy w ramach wszystkich czterech filarów strategii, obejmujące wprowadzenie przełomowych przepisów we wszystkich dziedzinach – od ochrony podmiotów krytycznych po zwiększenie cyberodporności. W międzyczasie jednak krajobraz zagrożeń dla bezpieczeństwa w Europie i w jej sąsiedztwie ciągle się zmienia. Ataki terrorystyczne, które miały miejsce w ostatnich dniach w jednej ze szkół we Francji i na ulicach Brukseli, wyraźnie przypominają o pilnej potrzebie dalszego dostosowywania i wzmacniania europejskiej architektury bezpieczeństwa. Zagrożenie stwarzane przez cyberataki jest coraz większe, również w miarę jak podmioty działające w złym zamiarze zajmują stanowisko w trwających konfliktach. Zagrożenia hybrydowe, w tym dezinformacja, nadal się nasilają. Europol uznał rosyjską wojnę napastniczą przeciwko Ukrainie za przyczynę znacznego nasilenia cyberataków na cele UE, przy czym poważne ataki są motywowane politycznie i koordynowane przez prorosyjskie grupy hakerów[2]. W ramach tych ataków zablokowano dostęp do internetu i doprowadzono do przerw w dostępie do kluczowych usług, takich jak sieci energetyczne[3].

Strategię w zakresie unii bezpieczeństwa opracowano w taki sposób, aby UE była bardziej odporna w obliczu zmieniającego się krajobrazu zagrożeń. Wydarzenia związane z kryzysami spowodowanymi pandemią i wojną pokazały, jak ważne jest podejście przyjęte w strategii, polegające na zapewnieniu spójności całego ekosystemu bezpieczeństwa UE i przezwyciężeniu barier oddzielających bezpieczeństwo fizyczne od cyfrowego, m.in. przez zwalczanie przestępczości zorganizowanej i terroryzmu oraz radykalizacji postaw.

Należy jednak zachować czujność i stale analizować, czego brakuje w podejmowanych działaniach mających zapewnić bezpieczeństwo obywateli Unii. W strategii określono obszary priorytetowe, w których Unia może wnieść wartość dodaną i pomóc państwom członkowskim w poprawie bezpieczeństwa wszystkich osób żyjących w Europie. Od czasu przyjęcia strategii podjęto wszystkie działania w niej określone i włączono nowe działania w odpowiedzi na bieżące zagrożenia bezpieczeństwa.

Ogólnie rzecz biorąc, w ramach strategii w zakresie unii bezpieczeństwa Komisja przedstawiła 36 inicjatyw ustawodawczych. W przypadku ponad połowy tych wniosków negocjacje międzyinstytucjonalne zakończyły się już przyjęciem solidnych nowych przepisów, jak opisano w tabeli w załączniku. Negocjacje Parlamentu Europejskiego i Rady w sprawie kilku kluczowych inicjatyw zaproponowanych przez Komisję pozostają jednak w toku. Ponieważ obecna kadencja parlamentarna dobiegnie końca wraz z wyborami europejskimi w czerwcu 2024 r., konieczne są szybkie prace nad tymi nierozstrzygniętymi dokumentami, tak aby obywatele mogli w pełni korzystać z unii bezpieczeństwa. W niniejszym szóstym sprawozdaniu z postępów prac w zakresie unii bezpieczeństwa skoncentrowano się zatem na

---

1 COM(2020) 605.

2 Rozproszone ataki typu „odmowa usługi” (atak typu DDoS): zob. sprawozdanie Europolu Spotlight pt. „Cyber-attacks: the apex of crime-as-a-service” („Cyberataki: szczyt zjawiska usług przestępczych”), 13 września 2023 r.

3 Podczas konfliktu w Ukrainie w dużej mierze wykorzystuje się złośliwe oprogramowania typu *wiper* do niszczenia danych i systemów, co na przykład miało wpływ na dostęp do internetu tysięcy abonentów w UE, a także w wyniku czego duże niemieckie przedsiębiorstwo energetyczne utraciło dostęp do zdalnego monitorowania ponad 5 800 turbin wiatrowych. „The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict” („Rola cyberprzestrzeni w rosyjskiej wojnie przeciwko Ukrainie: jej wpływ i konsekwencje w kontekście przyszłości konfliktu zbrojnego”), analiza Parlamentu Europejskiego, wrzesień 2023 r. – PE 702.594.

przedstawieniu tych kluczowych aktów ustawodawczych i nieustawodawczych, które Komisja przyjęła, ale których ukończenie i skuteczne wdrożenie wymaga dalszych działań.

Co się tyczy już uzgodnionych przepisów UE – korzyści z nich płynące będą odczuwalne dopiero wtedy, gdy zostaną one wprowadzone w życie. Dalsze prace muszą koncentrować się na ich prawidłowym i pełnym przetransponowaniu, wdrożeniu i stosowaniu przez państwa członkowskie. W 2023 r. Komisja nadal zapewniała realizację strategii UE w zakresie unii bezpieczeństwa, korzystając ze swoich uprawnień instytucjonalnych do wszczynania postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w każdym przypadku, w którym państwa członkowskie nie dokonały transpozycji przepisów UE lub zrobiły to nieprawidłowo.

W niniejszym sprawozdaniu podsumowano również obszary, w których działania państw członkowskich lub agencji UE mają kluczowe znaczenie dla realizacji celów. Agencje UE odgrywają kluczową rolę we wspieraniu realizacji inicjatyw w zakresie unii bezpieczeństwa, a ich obowiązki rozwinęły się w ostatnich latach. W niniejszym sprawozdaniu przedstawiono niektóre z nowych głównych zadań, które zostały im powierzone z myślą o zapewnieniu państwom członkowskim większego wsparcia we wdrażaniu kluczowych inicjatyw w ramach unii bezpieczeństwa.

Co więcej, sytuacja geopolityczna uwidoczniła, jak duże znaczenie dla bezpieczeństwa wewnętrznego Unii ma jej bezpieczeństwo zewnętrzne. Silniejsze ramy wewnętrzne UE w dziedzinie bezpieczeństwa nierozerwalnie wiążą się ze ściślejszymi partnerstwami i współpracą z państwami trzecimi. UE musi nadal aktywnie dążyć do tego, aby jej zaangażowanie na całym świecie przyczyniało się do zapewnienia bezpieczeństwa obywateli na jej terytorium.

II. Środowisko bezpieczeństwa, które wytrzyma próbę czasu

Cyberbezpieczeństwo i odporność infrastruktury krytycznej

W ramach unii bezpieczeństwa Unia zobowiązała się do zapewnienia wszystkim europejskim obywatelom i przedsiębiorstwom właściwej ochrony, zarówno w internecie, jak i poza nim, oraz do promowania otwartej, bezpiecznej i stabilnej cyberprzestrzeni. Rosnąca skala, częstotliwość i wpływ cyberincydentów stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych oraz dla rynku wewnętrznego. Rosyjska wojna napastnicza przeciwko Ukrainie jeszcze bardziej pogłębiła to zagrożenie, a obecne napięcia geopolityczne nasilają się wskutek ingerencji podmiotów powiązanych z państwem, przestępców i haktywistów. Sabotaż rurociągów Nord Stream, który miał miejsce ostatniej jesieni, pokazał, jak bardzo istotne sektory, takie jak energetyka, infrastruktura cyfrowa, transport i przestrzeń kosmiczna, zależą od odpornej infrastruktury krytycznej. Niedawny incydent dotyczący podmorskiego gazociągu i kabla telekomunikacyjnego w Estonii i Finlandii wskazuje, że należy zapewnić wysoki poziom gotowości do radzenia sobie z tego rodzaju sytuacjami. Chociaż przyczyna uszkodzenia pozostaje niejasna, a dochodzenia są w toku, wymiana informacji na różnych szczeblach między państwami członkowskimi i Komisją jest obiecująca. Zakłócenia te nie miały żadnego bezpośredniego wpływu na łączność internetową ani na bezpieczeństwo dostaw gazu na szczeblu europejskim lub lokalnym. Jest to oznaka poczynionych postępów i wzmożonych działań w zakresie gotowości podjętych w ostatnich miesiącach.

Aby zapewnić ochronę i odporność tych infrastruktur krytycznych, konieczne jest zatem funkcjonowanie jasnych i solidnych ram prawnych. W tym kontekście kluczowy przełom osiągnięto dzięki równoległemu przyjęciu zmienionej dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2)[4] oraz dyrektywy w sprawie odporności podmiotów krytycznych (dyrektywa CER)[5], które weszły w życie 16 stycznia 2023 r. Obecnie wzywa się państwa członkowskie do szybkiej i pełnej transpozycji tych podstawowych aktów prawnych, najpóźniej do 17 października 2024 r., w celu wprowadzenia solidnych unijnych ram ochrony unijnej infrastruktury krytycznej przed zagrożeniami fizycznymi i zagrożeniami cyberbezpieczeństwa.

W lipcu 2023 r. Komisja określiła w rozporządzeniu delegowanym Komisji usługi kluczowe w 11 sektorach objętych dyrektywą CER[6]. Kolejnym krokiem jest przeprowadzenie przez państwa członkowskie ocen ryzyka w odniesieniu do tych usług. W następstwie zalecenia Rady[7] z dnia 8 grudnia 2022 r. zintensyfikowano prace nad testami warunków skrajnych dotyczącymi infrastruktury krytycznej, począwszy od sektora energetycznego, oraz nad zacieśnieniem współpracy z NATO i kluczowymi krajami partnerskimi. Prace te doprowadziły do sporządzenia w czerwcu 2023 r. przez grupę zadaniową UE–NATO sprawozdania na temat odporności infrastruktury krytycznej, w którym przedstawiono obecne zagrożenia bezpieczeństwa związane z infrastrukturą krytyczną w czterech kluczowych sektorach (energia, transport, infrastruktura cyfrowa i przestrzeń kosmiczna) oraz zawarto zalecenia dotyczące zwiększenia odporności. Zalecenia, w tym dotyczące zwiększonej koordynacji, wymiany informacji i ćwiczeń, są obecnie wdrażane przez personel UE i NATO w kontekście zorganizowanego dialogu na temat odporności.

Jednocześnie 6 września 2023 r. Komisja przyjęła wniosek[8] dotyczący zalecenia Rady w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym. W dniu 4 października 2023 r. zorganizowano ćwiczenie w formie opartej na scenariuszach dyskusji na temat tego planu, aby przetestować, w jaki sposób będzie on stosowany w praktyce, oraz zapewnić wkład w bieżące negocjacje toczące się w sprawie wniosku w Radzie.

W odpowiedzi na apele Rady[9] Komisja, wysoki przedstawiciel i grupa współpracy NIS przeprowadzają oceny ryzyka i opracowują scenariusze ryzyka z perspektywy cyberbezpieczeństwa. Prace te koncentrują się początkowo na sektorach telekomunikacji i energii elektrycznej. Zaangażowanie wszystkich odpowiednich agencji i sieci, cywilnych i wojskowych, sprawia, że po raz pierwszy możliwe jest przeprowadzenie kompleksowej i pluralistycznej ogólnounijnej oceny. Będzie ona uzupełnieniem skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzanych na podstawie dyrektywy NIS 2 oraz ocen ryzyka i testów warunków skrajnych infrastruktury krytycznej w sektorach energetycznym, sektorach łączności cyfrowej, transportu i sektorze kosmicznym. Na potrzeby zapewnienia koordynacji i spójności działania te powinny wzajemnie się uzupełniać, aby na ich podstawie można było wypracować standardowe podejście i określić

[4] Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii oraz dyrektywa (UE) 2018/1972 (dyrektywa NIS 2).

[5] 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.

[6] C(2023) 4878.

[7] Zalecenie Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

[8] COM(2023) 526.

[9] Konkluzje Rady z dnia 23 maja 2022 r. o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i wezwanie z Nevers z dnia 9 marca 2022 r. do wzmocnienia zdolności UE w zakresie cyberbezpieczeństwa.

kierunek rozwoju przyszłych ćwiczeń. Powodzenie tych działań będzie teraz zależało od aktywnego zaangażowania państw członkowskich.

Funkcjonowanie gospodarek i społeczeństw jest w coraz większym stopniu uzależnione od usług i danych związanych z przestrzenią kosmiczną, zwłaszcza w dziedzinie bezpieczeństwa i obrony. Przestrzeń kosmiczna staje się obszarem coraz bardziej spornym, a jej znaczenie dla bezpieczeństwa wzrosło, zwłaszcza w następstwie rosyjskiej inwazji na Ukrainę. W marcu 2023 r. przyjęto strategię kosmiczną UE na rzecz bezpieczeństwa i obrony, aby wzmocnić strategiczne podejście UE i jej autonomię w domenie kosmicznej. Jako kluczowe działanie wynikające z tej strategii Komisja Europejska zaproponuje w 2024 r. unijne prawo kosmiczne regulujące bezpieczeństwo, zrównoważoność i odporność/bezpieczeństwo działań związanych z przestrzenią kosmiczną w UE.

Jeśli chodzi o wymiar zewnętrzny, bezpieczna infrastruktura stanowi podstawę odporności globalnej gospodarki i łańcuchów dostaw[10], w związku z czym unijna strategia Global Gateway obejmuje silny wymiar bezpieczeństwa. Podobnie, biorąc pod uwagę wzajemne powiązania między infrastrukturą UE a infrastrukturą krajów partnerskich, dalsza współpraca międzynarodowa ma zasadnicze znaczenie w kontekście wzmocnienia globalnej cyberodporności i wspierania wolnej, otwartej, bezpiecznej i chronionej cyberprzestrzeni.

Akt dotyczący cyberodporności

W kontekście europejskiego cyberbezpieczeństwa kluczowe znaczenie ma zapewnienie konsumentom i przedsiębiorstwom możliwości korzystania z bezpiecznych produktów cyfrowych. Komisja uwzględniła tę potrzebę we wniosku dotyczącym aktu dotyczącego cyberodporności[11], przyjętym 15 września 2022 r. W drodze tego aktu zostaną wprowadzone obowiązkowe horyzontalne wymogi cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi, stosowane przez okres pięciu lat lub przez cały okres eksploatacji produktu (w zależności od tego, który z tych okresów jest krótszy). W ten sposób zostaną stworzone warunki do projektowania i opracowywania bezpiecznych produktów z elementami cyfrowymi przez zapewnienie, aby sprzęt i oprogramowanie były wprowadzane do obrotu z jak najmniejszą liczbą podatności. Będzie to kluczowy krok w podnoszeniu europejskich standardów w zakresie cyberbezpieczeństwa we wszystkich dziedzinach i prawdopodobnie stanie się międzynarodowym punktem odniesienia, przynosząc wyraźne korzyści unijnej branży cyberbezpieczeństwa na rynkach światowych. W lipcu 2023 r. Parlament Europejski i Rada przyjęły swoje stanowiska, a negocjacje powinny przebiegać sprawnie.

Certyfikacja cyberbezpieczeństwa odgrywa również kluczową rolę w zwiększaniu zaufania do produktów i usług ICT, gdyż zapewnia odpowiedni poziom cyberbezpieczeństwa i sprawia, że konsumenci, przedsiębiorstwa i organy mogą dokonywać świadomych wyborów. Trwają prace nad certyfikacją cyberbezpieczeństwa – obecnie w ramach procedury komitetowej prowadzona jest ocena unijnego systemu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach. Proponowany unijny system certyfikacji bezpieczeństwa w chmurze (EUCS) jest obecnie przygotowywany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i jest omawiany na forum Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa. Intensywna współpraca z ekspertami z różnych sektorów, konsumentami i dostawcami powinna skutkować wypracowaniem solidnego podejścia prawnego i technicznego zapewniającego niezbędne gwarancje bezpieczeństwa zgodne z prawem Unii, zobowiązaniami międzynarodowymi i zobowiązaniami w ramach WTO. ENISA przygotowuje ponadto propozycję unijnego programu w zakresie sieci 5G oraz unijny portfel tożsamości cyfrowej

[10] JOIN(2021) 30.
[11] COM(2022) 454.

(EUIDW). W kontekście zwiększenia ogólnego bezpieczeństwa produktów ICT, usług ICT i procesów ICT zasadnicze znaczenie mają wspólne działania podejmowane przez wszystkie państwa członkowskie.

Rozporządzenia dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa odnoszące się do instytucji, organów, urzędów i agencji Unii

Prace nad zaproponowanymi razem w marcu 2022 r. rozporządzeniami regulującymi cyberbezpieczeństwo i bezpieczeństwo informacji w zakresie własnych instytucji Unii przebiegają w różnym tempie. W czerwcu ubiegłego roku osiągnięto porozumienie polityczne dotyczące rozporządzenia w sprawie cyberbezpieczeństwa, które umożliwia poprawę stanu cyberbezpieczeństwa wszystkich instytucji, organów, urzędów i agencji Unii i odzwierciedla wagę, jaką UE przywiązuje do szybkiego wdrożenia tego wniosku. W tej sytuacji szczególnie niepokojące są nieoczekiwanie wolne postępy poczynione w zakresie równoległego wniosku w sprawie bezpieczeństwa informacji, który ma zasadnicze znaczenie dla zapewnienia kompletności solidnych ram legislacyjnych odnoszących się do instytucji, organów, urzędów i agencji Unii. Oba wnioski powinny zostać przyjęte przed wyborami do Parlamentu Europejskiego w celu potwierdzenia wiarygodności europejskiej administracji i jej odporności w aktualnej sytuacji geopolitycznej. Za pomocą minimalnego zestawu przepisów i norm bezpieczeństwa informacji obowiązujących wszystkie instytucje, organy, urzędy i agencje Unii zapewniono by pewność na potrzeby wszystkich zaangażowanych stron oraz spójną ochronę ich informacji – zarówno informacji niejawnych UE, jak i informacji jawnych – przed zmieniającymi się zagrożeniami. Łącznie te nowe przepisy stanowiłyby stabilną podstawę bezpiecznej wymiany informacji między instytucjami, organami, urzędami i agencjami Unii oraz z państwami członkowskimi, przy zastosowaniu znormalizowanych praktyk i środków służących ochronie przepływu informacji. Stanowią one zatem odpowiedź na liczne apele Rady o zwiększenie odporności instytucji, organów, urzędów i agencji Unii i o lepszą ochronę unijnego procesu decyzyjnego przed ingerencją w złym zamiarze.

Akt w sprawie cybersolidarności

W oparciu o już istniejące solidne ramy strategiczne, polityczne i legislacyjne zaproponowany unijny akt w sprawie cybersolidarności[12], przyjęty przez Komisję 18 kwietnia 2023 r., przyczyniłby się do poprawy wykrywania cyberzagrożeń oraz podwyższenia odporności i gotowości na wszystkich szczeblach unijnego ekosystemu cyberbezpieczeństwa. Cele te byłyby realizowane za pośrednictwem trzech głównych działań:

1) wprowadzenie ***europejskiej tarczy cyberbezpieczeństwa*** w celu zbudowania i wzmocnienia wspólnych zdolności w zakresie wykrywania i orientacji sytuacyjnej. W skład tarczy wchodziłyby krajowe centra monitorowania bezpieczeństwa („krajowe SOC") oraz transgraniczne centra monitorowania bezpieczeństwa („transgraniczne SOC").
2) stworzenie ***mechanizmu cyberkryzysowego***, aby wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie i w natychmiastowym usuwaniu ich skutków. Wsparcie w reagowaniu na incydenty obejmowałoby unijną rezerwę cyberbezpieczeństwa, którą udostępniano by również europejskim instytucjom, organom, urzędom i agencjom Unii oraz państwom trzecim stowarzyszonym w ramach programu „Cyfrowa Europa", jeżeli zostało to przewidziane w zawartym przez te państwa układzie o stowarzyszeniu w ramach programu „Cyfrowa Europa";

[12] COM(2023) 209.

3) ustanowienie ***europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie*** na potrzeby przeglądu i oceny poważnych incydentów lub incydentów na dużą skalę. Sprawozdanie z przeglądu incydentu będzie koordynowane i przygotowywane przez ENISA.

Rozpoczęto dyskusje w Radzie i w Parlamencie Europejskim. Zakończenie negocjacji przed końcem obecnej kadencji Parlamentu Europejskiego stanowiłoby istotny bodziec, jeżeli chodzi o działania na rzecz ochrony obywateli i przedsiębiorstw w całej Unii.

Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa

Zagrożenia cyberbezpieczeństwa narastają, a UE pilnie potrzebuje specjalistów, którzy mają umiejętności i kompetencje pozwalające na zapobieganie cyberatakom, ich wykrywanie i powstrzymywanie oraz ochronę przed cyberatakami. Aktualnie szacuje się, że potrzeba 883 000 specjalistów ds. cyberbezpieczeństwa, zaś liczba nieobsadzonych stanowisk w 2022 r. wahała się w przedziale od 260 000 do 500 000. Należy zachęcać wszystkie grupy społeczne do pomocy w wypełnieniu tej luki, przy czym należy zauważyć, że w 2022 r. kobiety stanowiły jedynie 20 % absolwentów kierunków związanych z cyberbezpieczeństwem i 19 % specjalistów ds. technologii informacyjno-komunikacyjnych. W ramach Europejskiego Roku Umiejętności 2023 Komisja przyjęła 18 kwietnia 2023 r.[13] inicjatywę, z zadowoleniem przyjętą przez państwa członkowskie[14], dotyczącą utworzenia Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa z myślą o wyeliminowaniu niedoboru talentów w tej dziedzinie. Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa połączyłaby istniejące inicjatywy dotyczące umiejętności w dziedzinie cyberbezpieczeństwa i przyczyniłaby się do poprawy koordynacji. Komisja zachęca państwa członkowskie, władze regionalne i lokalne, a także europejskie podmioty publiczne, do przyjęcia specjalnych strategii lub inicjatyw dotyczących umiejętności w dziedzinie cyberbezpieczeństwa lub do włączenia kwestii umiejętności w dziedzinie cyberbezpieczeństwa do odpowiednich strategii lub inicjatyw o szerszym zakresie (np. w zakresie cyberbezpieczeństwa, umiejętności cyfrowych, zatrudnienia itp.). Zaangażowanie prywatnych zainteresowanych stron będzie miało również zasadnicze znaczenie w kontekście zmniejszenia luki w umiejętnościach w dziedzinie cyberbezpieczeństwa i związanego z nią niedoboru siły roboczej w Europie.

Drony

Kolejnym rosnącym zagrożeniem dla przestrzeni publicznej i infrastruktury krytycznej jest wykorzystywanie dronów w złym zamiarze. Incydenty z udziałem dronów stają się coraz częstsze w Unii i poza nią, a rozwiązania w zakresie przeciwdziałania dronom stanowią kluczowe narzędzie dla organów ścigania i innych organów publicznych w Unii, a także dla prywatnych operatorów infrastruktury krytycznej. Jednocześnie zgodne z prawem wykorzystywanie dronów wnosi istotny wkład w dwojaką transformację – ekologiczną i cyfrową[15]. Jak zapowiedziano w strategii dotyczącej dronów 2.0, przyjętej w listopadzie 2022 r., Komisja przyjmuje dziś komunikat w sprawie przeciwdziałania potencjalnym zagrożeniom stwarzanym przez bezzałogowe statki powietrzne, poparty dwoma podręcznikami zawierającymi praktyczne wytyczne na temat kluczowych aspektów technicznych[16]. Inicjatywa ta służy zapewnieniu kompleksowych i zharmonizowanych ram polityki, wypracowaniu jednolitego zrozumienia obowiązujących przepisów w celu sprostania zagrożeniom, jakie mogą stwarzać bezzałogowe statki powietrzne, oraz przystosowaniu się do szybkiego rozwoju

[13] COM(2023) 207.
[14] Konkluzje Rady z dnia 22 maja 2023 r. w sprawie polityki UE w zakresie cyberobrony.
[15] COM(2022) 652.
[16] COM(2023) 659.

technologii. Państwa członkowskie i odpowiednie podmioty prywatne zachęca się do ścisłej współpracy z Komisją w celu zapewnienia pełnego wdrożenia tej inicjatywy.

Bezpieczeństwo morskie i ochrona lotnictwa

Nielegalne działania, takie jak piractwo, zbrojne napaści na statki, przemyt migrantów i handel ludźmi, handel bronią i narkotykami, a także terroryzm, nadal stanowią wyzwania dla bezpieczeństwa morskiego potęgowane przez zmieniające się zagrożenia, w tym ataki hybrydowe i cyberataki. 10 marca 2023 r. Komisja i wysoki przedstawiciel przyjęli wspólny komunikat aktualizujący strategię Unii Europejskiej w zakresie bezpieczeństwa morskiego[17], którą należy teraz wdrożyć zgodnie z zaktualizowanym planem działania.

W obszarze ochrony lotnictwa 2 lutego 2023 r. Komisja przyjęła dokument roboczy służb Komisji pt. „Praca na rzecz wzmocnionej i odporniejszej polityki ochrony lotnictwa”[18], który zawiera ambitny program mający na celu 1) modernizację struktury regulacyjnej w zakresie ochrony lotnictwa, (2) wspieranie rozwoju i wdrażania bardziej innowacyjnych rozwiązań; oraz 3) zaktualizowanie podstaw ochrony lotnictwa, tak aby unijne porty lotnicze mogły w pełni korzystać z nowych i najnowocześniejszych technologii w celu przeciwdziałania najbardziej priorytetowym zagrożeniom. W ciągu dwóch lat należy wdrożyć czternaście działań przewodnich.

Komisja wzywa Parlament Europejski i Radę do pilnego zakończenia negocjacji, w każdym razie jeszcze przed końcem kadencji obecnego Parlamentu Europejskiego, dotyczących następujących dokumentów:

- wniosku w sprawie europejskiego aktu dotyczącego cyberodporności;
- wniosku dotyczącego europejskiego aktu w sprawie cybersolidarności;
- proponowanego rozporządzenia w sprawie bezpieczeństwa informacji w zakresie instytucji, organów, urzędów i agencji Unii.

Komisja wzywa państwa członkowskie do:

- priorytetowego traktowania transpozycji dyrektywy w sprawie odporności podmiotów krytycznych, a także testowania warunków skrajnych w przypadku infrastruktury krytycznej w sektorze energetycznym;
- przyjęcia zalecenia Rady w sprawie planu skoordynowanego reagowania na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym;
- pełnej i pilnej transpozycji dyrektywy NIS 2 w celu zwiększenia cyberbezpieczeństwa podmiotów kluczowych i ważnych;
- aktywnego angażowania się w przeprowadzanie oszacowań ryzyka w cyberbezpieczeństwie i tworzenie scenariuszy ryzyka w odniesieniu do infrastruktury krytycznej i łańcuchów dostaw;
- prowadzenia działań następczych w związku z Akademią Umiejętności w dziedzinie Cyberbezpieczeństwa przy silnym zaangażowaniu na szczeblu europejskim i w ramach specjalnych krajowych strategii lub inicjatyw dotyczących umiejętności w zakresie cyberbezpieczeństwa, z udziałem kluczowych zainteresowanych stron, w tym władz regionalnych i lokalnych;
- współpracy z odpowiednimi podmiotami prywatnymi i Komisją w celu zapewnienia realizacji wszystkich działań wymienionych w komunikacie w sprawie

[17] JOIN(2023) 8.
[18] SWD(2023) 37.

przeciwdziałania potencjalnym zagrożeniom stwarzanym przez bezzałogowe statki powietrzne;
- wdrożenia planu działania dotyczącego strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego i regularnego składania sprawozdań z osiągnięć;
- wdrożenia 14 działań przewodnich określonych w celu poprawy ochrony lotnictwa.

III. Działanie w obliczu zmieniających się zagrożeń

Nowe napięcia geopolityczne wyraźnie świadczą o tym, że zagrożenie bezpieczeństwa UE nie tylko nasilają się, ale również są coraz bardziej zmienne, na co wskazuje hybrydowy charakter wielu zagrożeń. W ramach zapewnienia bezpieczeństwa należy również reagować na zmiany społeczne i technologiczne. Wskutek pandemii COVID-19 cyberprzestępcy zyskali nowe możliwości, a w szczególności wzrosło zagrożenie umieszczania w internecie materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych. Przestępcy i podmioty działające w złym zamiarze zawsze są gotowi do wykorzystywania osiągnięć technologicznych. W obliczu tego typu często złożonych i wielowymiarowych zagrożeń konieczne są zdecydowane i spójne działania UE.

Rozporządzenie w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych w internecie

Przeprowadzona przez Europol ocena zagrożenia zorganizowaną przestępczością internetową wykazała, że w 2022 r. doszło do nasilenia się zjawiska wykorzystywania seksualnego i niegodziwego traktowania dzieci w celach seksualnych pod względem częstotliwości i powagi tego procederu, a sprawcy nadal wykorzystują techniczne możliwości w celu ukrycia swoich działań i tożsamości[19]. Obecny system oparty na dobrowolnym wykrywaniu i zgłaszaniu przez przedsiębiorstwa okazał się niewystarczający do ochrony dzieci. Rozporządzenie tymczasowe umożliwia dobrowolne wykrywanie i zgłaszanie przez przedsiębiorstwa, pod warunkiem że jest to zgodne z ogólnym rozporządzeniem o ochronie danych (RODO). Rozporządzenie to przestanie obowiązywać w sierpniu 2024 r. W maju 2022 r. Komisja przedstawiła wniosek dotyczący rozporządzenia[20], aby rozwiązać problem niewłaściwego wykorzystywania usług online do celów niegodziwego traktowania dzieci w celach seksualnych. W proponowanych ramach duży nacisk kładzie się na zapobieganie. Przedsiębiorstwa będą zobowiązane do oceny ryzyka wykorzystania ich systemów do niegodziwego traktowania dzieci w celach seksualnych oraz do podejmowania środków zapobiegawczych. W ostateczności wyłącznie w przypadku występowania znacznego ryzyka sądy krajowe lub niezależne organy administracyjne mogłyby wydawać ukierunkowane nakazy wykrywania skierowane do dostawców usług. Dostawcom usług łatwiej będzie podejmować działania dzięki nowemu niezależnemu Unijnemu Centrum, które będzie pełnić rolę ośrodka gromadzącego wiedzę ekspercką, dostarczać wiarygodne informacje na temat zidentyfikowanych materiałów, otrzymywać i analizować dokonywane przez dostawców zgłoszenia dotyczące przypadków niegodziwego traktowania dzieci w celach seksualnych w internecie w celu identyfikowania błędnych zgłoszeń, a także udzielać wsparcia ofiarom. Konieczne jest jak najszybsze przyjęcie i wdrożenie nowych przepisów w celu ochrony dzieci przed dalszym niegodziwym traktowaniem, zapobiegania ponownemu pojawianiu się

[19] Europol (2023), ocena zagrożenia zorganizowaną przestępczością internetową (IOCTA) 2023.
[20] COM(2022) 209.

materiałów w internecie oraz stawiania sprawców przed wymiarem sprawiedliwości. Obecnie trwają negocjacje w Radzie i Parlamencie służące osiągnięciu porozumienia w sprawie tego aktu przed końcem obecnej kadencji Parlamentu.

Dyrektywa w sprawie zwalczania przemocy wobec kobiet i przemocy domowej

Cyberprzemoc wobec kobiet, m.in. w kontekście przemocy domowej, stała się nową formą takiej przemocy, która za pośrednictwem internetu i narzędzi IT rozprzestrzenia się ponad granicami poszczególnych państw członkowskich. W marcu 2022 r. Komisja zaproponowała dyrektywę w sprawie zwalczania przemocy wobec kobiet i przemocy domowej, w tym szczegółowe przepisy dotyczące cyberprzemocy oraz środki mające na celu zniwelowanie luk w zakresie ochrony, dostępu do wymiaru sprawiedliwości i zapobiegania. W przypadku wczesnego przyjęcia i wdrożenia państwa członkowskie zyskałyby dodatkowe narzędzia do zwalczania tej formy przestępczości. Współprawodawcy rozpoczęli negocjacje międzyinstytucjonalne w lipcu 2023 r. i zamierzają je zakończyć przed końcem obecnej kadencji Parlamentu Europejskiego.

Cyberbezpieczeństwo sieci 5G

Bezpieczeństwo sieci 5G jest jednym z głównych priorytetów Komisji i istotnym elementem jej strategii w zakresie unii bezpieczeństwa. Sieci 5G są infrastrukturą centralną, która stanowi podstawę szerokiej gamy usług koniecznych do funkcjonowania rynku wewnętrznego oraz niezbędnych funkcji społecznych i gospodarczych. 15 czerwca 2023 r. władze państw członkowskich UE reprezentowane w grupie współpracy NIS, przy wsparciu Komisji i ENISA, opublikowały drugie sprawozdanie z postępów we wdrażaniu unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Zgodnie z tym sprawozdaniem 24 państwa członkowskie przyjęły lub przygotowują środki ustawodawcze przyznające organom krajowym uprawnienia do przeprowadzania oceny dostawców i wydawania ograniczeń, a 10 państw członkowskich nałożyło takie ograniczenia. Konieczne są jednak dalsze działania, aby uniknąć podatności całej Unii, co mogłoby mieć poważne negatywne skutki dla bezpieczeństwa indywidualnych użytkowników i przedsiębiorstw w całej Unii oraz dla unijnej infrastruktury krytycznej. Wszystkie państwa członkowskie muszą niezwłocznie wdrożyć zestaw narzędzi. W tym samym dniu Komisja przyjęła komunikat w sprawie wdrożenia zestawu narzędzi przez państwa członkowskie oraz w sprawie komunikacji instytucjonalnej Komisji i unijnych działań w zakresie finansowania. Uwypukliło to poważne obawy dotyczące ryzyka dla bezpieczeństwa UE stwarzanego przez dostawców urządzeń komunikacyjnych sieci telefonii ruchomej Huawei i ZTE. W tym kontekście Komisja wprowadza środki, aby uniknąć narażenia swojej komunikacji instytucjonalnej na działanie sieci ruchomych, w których dostawcami są Huawei i ZTE. Zamówienia nie będą obejmowały nowych usług łączności opartych na sprzęcie od tych dostawców, a Komisja będzie współpracować z państwami członkowskimi i operatorami telekomunikacyjnymi, aby zapewnić stopniowe wycofywanie tych dostawców z istniejących usług łączności w siedzibach Komisji. Komisja bada również, w jaki sposób uwzględnić tę decyzję w odpowiednich unijnych programach i instrumentach finansowania, w pełnej zgodności z prawem Unii.

Dostęp do danych w celu skutecznego ścigania przestępstw

W dzisiejszej erze cyfrowej prawie każde przestępstwo ma komponent cyfrowy. Do celów przestępczych wykorzystuje się również technologie i narzędzia, w tym te, które są niezbędne, aby zaspokoić potrzeby naszego społeczeństwa w zakresie cyberbezpieczeństwa oraz zagwarantować mu ochronę danych i prywatność. W rezultacie utrzymanie skutecznego ścigania przestępstw w całej UE w celu ochrony bezpieczeństwa publicznego oraz zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich

ścigania staje się coraz trudniejsze. Choć podjęto znaczne starania na szczeblu unijnym i krajowym, obejmujące m.in. prawodawstwo, a także inicjatywy na rzecz budowania zdolności i innowacji, w dalszym ciągu stoimy przed pewnymi wyzwaniami natury prawnej i technicznej. Komisja, w porozumieniu z prezydencją Rady, powołała grupę ekspertów wysokiego szczebla ds. dostępu do danych z myślą o skutecznej pracy organów ścigania, aby zapewnić platformę współpracy dla szerokiego grona zainteresowanych stron i ekspertów umożliwiającą im przeanalizowanie problemów, z którymi mierzą się praktycy organów ścigania w sprawach karnych (np. szyfrowanie, zatrzymywanie danych, sieć 5G i normalizacja). Komisja oczekuje, że do czerwca 2024 r. grupa wysokiego szczebla sformułuje wyważone, konkretne i możliwe do zrealizowania zalecenia odzwierciedlające złożoność tych kwestii, m.in. z punktu widzenia cyberbezpieczeństwa i ochrony danych. Zachęca się zatem państwa członkowskie i uczestniczących ekspertów do aktywnego zaangażowania się w ten proces i do pracy nad skutecznymi, zgodnymi z prawem i powszechnie akceptowanymi rozwiązaniami.

Zagrożenia hybrydowe

W obliczu sytuacji geopolitycznej, w której zagrożenia hybrydowe stają się coraz bardziej złożone i zaawansowane, w unijnym Strategicznym kompasie na rzecz bezpieczeństwa i obrony[21] („Strategiczny kompas") przedstawiono wspólną ocenę zagrożeń i wyzwań, przed którymi stoi Unia, a także strategiczny plan działania. Coraz częściej dochodzi do szkodliwych działań w cyberprzestrzeni ze strony państw i podmiotów niepaństwowych, m.in. w kontekście wojny przeciwko Ukrainie, co dodatkowo uwydatnia znaczenie cyberprzestrzeni jako obszaru polityki zagranicznej i bezpieczeństwa. Potencjalne ryzyko szkodliwych działań i dezinformacji wymaga szczególnej czujności w okresach wyborczych, w tym w okresie poprzedzającym wybory do Parlamentu Europejskiego w 2024 r.

Mając na uwadze wysokie ryzyko efektu mnożnikowego, UE nadal rozwijała działania na rzecz budowania zdolności cyfrowych i wspierała partnerstwa z państwami trzecimi, w tym za pomocą specjalnych dialogów w sprawach cyberprzestrzeni, tak aby aktywnie wspierać ogólną odporność UE. Opracowano, zmieniono i usprawniono szereg narzędzi w celu zwiększenia zdolności Unii do skutecznego reagowania na zagrożenia hybrydowe, jak opisano w siódmym sprawozdaniu z postępów w działaniach w zakresie zagrożeń hybrydowych, opublikowanym w dniu 14 września 2023 r.[22] Prace te obejmują:

- unijny zestaw narzędzi do przeciwdziałania zagrożeniom hybrydowym zapewniający ramy skoordynowanej i świadomej reakcji na zagrożenia i kampanie hybrydowe;
- trwające prace nad utworzeniem unijnych zespołów szybkiego reagowania na zagrożenia hybrydowe, zapewniających w krótkim czasie dostosowane wsparcie dla państw członkowskich, krajów partnerskich oraz misji i operacji w dziedzinie wspólnej polityki bezpieczeństwa i obrony (WPBiO);
- zmieniony unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym („unijny podręcznik taktyczny")[23], w którym opisano unijne procesy i struktury pozwalające reagować na zagrożenia i kampanie hybrydowe;
- zmienione wytyczne dotyczące wdrażania ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni[24] („zestaw narzędzi dla dyplomacji cyfrowej"), które umożliwiają opracowanie trwałych, dostosowanych do potrzeb, spójnych i skoordynowanych strategii przeciwko podmiotom nieustannie powodującym zagrożenia cyberbezpieczeństwa;

[21] Dokument Rady 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] Dokument 10289/23 z dnia 8 czerwca 2023 r.

- zestaw narzędzi służących przeciwdziałaniu zagranicznym manipulacjom informacjami i ingerencjom w informacje, którego celem jest usprawnienie istniejących narzędzi unijnych służących do zapobiegania zagranicznym manipulacjom informacjami i ingerencjom w informacje, powstrzymywania ich i reagowania na nie;
- polityka UE w zakresie cyberobrony[25] mająca na celu zwiększenie zdolności cyberobronnych UE, poprawę orientacji sytuacyjnej i koordynację całego zakresu dostępnych możliwości obronnych w celu wzmocnienia odporności, reagowania na cyberataki oraz zapewnienia solidarności i wzajemnej pomocy.

W związku z powyższym zachęca się państwa członkowskie do podtrzymywania i zacieśniania współpracy w tej dziedzinie przez zapewnienie skutecznego wdrożenia wyżej wymienionych zestawów narzędzi, w tym prowadzenie regularnych ćwiczeń, oraz osiągnięcie porozumienia co do koncepcji zespołów szybkiego reagowania na zagrożenia hybrydowe, tak aby opracować wytyczne dotyczące dalszych kroków w kierunku utworzenia tych zespołów.

Sztuczna inteligencja w kontekście ścigania przestępstw

Sztuczna inteligencja (AI) szybko stała się wszechobecnym elementem codziennego życia. Wpływ wykorzystania AI na cyberprzestępczość i cyberbezpieczeństwo nie jest jeszcze w pełni znany, ale bez wątpienia przyniesie nowe wyzwania. Chociaż AI – gdy jest wykorzystywana w sposób bezpieczny i kontrolowany – może przynieść korzyści, może też być niebezpieczna, gdy znajdzie się w rękach podmiotów działających w złym zamiarze, może np. pomagać przestępcom ukrywać swoją tożsamość w przypadku przestępstw takich jak terroryzm czy niegodziwe traktowanie dzieci w celach seksualnych. Ważne jest zatem, aby organy na bieżąco informowały o rozwoju sytuacji, co pozwoli zapobiegać nadużyciom i reagować na niewłaściwe wykorzystywanie[26]. Rozwiązanie tych kwestii stanowi cel negocjacji dotyczących proponowanego aktu w sprawie sztucznej inteligencji, które weszły już w decydujący etap, a współprawodawcy omawiają obecnie kwestie techniczne i polityczne dotyczące interakcji z tą technologią w nadchodzących latach. Zasadnicze znaczenie będzie miało wypracowanie zrównoważonych rozwiązań, zwłaszcza w odniesieniu do zastosowań wysokiego ryzyka, w tym w obszarze ścigania przestępstw.

Komisja wzywa Parlament Europejski i Radę do pilnego zakończenia negocjacji międzyinstytucjonalnych, w każdym razie jeszcze przed końcem kadencji obecnego Parlamentu Europejskiego, dotyczących następujących rozpatrywanych dokumentów:

- wniosek dotyczący rozporządzenia w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych w internecie;
- wniosek dotyczący dyrektywy w sprawie zwalczania przemocy wobec kobiet i przemocy domowej;
- wniosek dotyczący rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji).

Komisja wzywa państwa członkowskie do:

- bezzwłocznego pełnego wdrożenia unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G;

[25] JOIN(2022) 49.

[26] Zob. na przykład sprawozdanie Europolu opublikowane 17 kwietnia 2023 r.: „ChatGPT – the impact of Large Language Models on Law Enforcement" [„ChatGPT – wpływ dużych modeli językowych na ściganie przestępstw"].

- wspierania prac grupy ekspertów wysokiego szczebla ds. dostępu do danych z myślą o skutecznej pracy organów ścigania w celu sformułowania jasnych, konkretnych i możliwych do zrealizowania zaleceń, tak aby w proporcjonalny sposób sprostać obecnym i przewidywanym wyzwaniom;
- podjęcia działań, we współpracy z wysokim przedstawicielem, w celu zapewnienia skutecznego wdrożenia unijnego zestawu narzędzi do przeciwdziałania zagrożeniom hybrydowym, zmienionego zestawu narzędzi dla dyplomacji cyfrowej i zestawu narzędzi służących przeciwdziałaniu zagranicznym manipulacjom informacjami i ingerencjom w informacje, w tym za pomocą regularnych ćwiczeń i z uwzględnieniem globalnej dynamiki;
- osiągnięcia porozumienia w sprawie koncepcji zespołów szybkiego reagowania na zagrożenia hybrydowe.

IV. Ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną

Należy zdawać sobie sprawę z nieustannego ryzyka, że wydarzenia globalne lub lokalne wywołają nowe ogniska terroryzmu. Jednocześnie do najpoważniejszych zagrożeń dla bezpieczeństwa UE należą przestępczość zorganizowana i nielegalny obrót środkami odurzającymi. W celu zintensyfikowania wspólnych działań na szczeblu Unii w walce z tymi zagrożeniami prowadzone są wspólne prace nad wdrożeniem unijnej strategii zwalczania przestępczości zorganizowanej[27], Strategii UE w zakresie zwalczania handlu ludźmi[28], agendy i planu działania UE w zakresie środków odurzających[29] oraz planu dla UE w dziedzinie zwalczania terroryzmu[30]. Aby jednak zareagować na niepokojąco pogarszającą się sytuację w zakresie przestępczości zorganizowanej i nielegalnego obrotu środkami odurzającymi, konieczne jest dalsze zintensyfikowanie działań państw członkowskich i UE w celu wzmocnienia naszej zbiorowej reakcji na aktywność siatek przestępczych i lepszej ochrony ofiar przestępstw, a równolegle z niniejszym sprawozdaniem publikowany jest unijny plan działania na rzecz zwalczania nielegalnego obrotu środkami odurzającymi i przestępczości zorganizowanej[31].

W dziedzinie zwalczania terroryzmu UE usprawnia również swój zestaw narzędzi zewnętrznych[32] za pomocą pełnego wykorzystania dialogów wysokiego szczebla w zakresie walki z terroryzmem oraz sieci ekspertów ds. bezpieczeństwa/zwalczania terroryzmu w delegaturach Unii, a także przez swoje zaangażowanie na forach wielostronnych, w tym jako współprzewodniczący Światowego Forum na rzecz Zwalczania Terroryzmu.

Nielegalny obrót środkami odurzającymi

Dzięki nowemu mandatowi Agencji Unii Europejskiej ds. Narkotyków, który będzie obowiązywać od lipca 2024 r., UE będzie lepiej przygotowana do rozwiązania złożonego

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] Zgodnie z apelem zawartym w Strategicznym kompasie i w konkluzjach Rady w sprawie zewnętrznego wymiaru stale ewoluującego zagrożenia terroryzmem i brutalnym ekstremizmem, przyjętych w czerwcu 2022 r.

problemu w zakresie bezpieczeństwa i zdrowia, dotykającego miliony ludzi w UE i na świecie. Komisja dokonuje również przeglądu[33] przepisów dotyczących prekursorów narkotyków[34], aby zająć się głównymi wyzwaniami określonymi w ocenie z 2020 r.[35], w której podkreślono potrzebę sprostania wyzwaniom, jakie stwarzają projektowane prekursory narkotyków[36] w celu ograniczenia podaży nielegalnych środków odurzających.

W obliczu bezprecedensowego wzrostu liczby niedozwolonych środków odurzających dostępnych w Europie należy jednak wzmóc walkę z nielegalnym obrotem środkami odurzającymi we współpracy z partnerami międzynarodowymi. Konieczne są dodatkowe działania ze strony państw członkowskich i UE, które pozwolą rozbić siatki przestępcze i zapewnić lepszą ochronę ofiar przestępstw. Komisja przedstawia dziś unijny plan działania na rzecz zwalczania nielegalnego obrotu środkami odurzającymi i przestępczości zorganizowanej. Określono w nim 17 działań w czterech obszarach priorytetowych: wzmocnienie odporności centrów logistycznych za pomocą sojuszu portów europejskich, rozbijanie siatek przestępczych, intensyfikacja działań zapobiegawczych oraz zacieśnienie współpracy z partnerami międzynarodowymi. Działania te mają zostać wdrożone w latach 2024 i 2025.

Broń palna

Nielegalny handel bronią sprzyja rozwojowi przestępczości zorganizowanej w UE i w jej sąsiedztwie. Szacuje się, że w UE w rękach prywatnych znajduje się aż 35 mln sztuk nielegalnej broni palnej, a około 630 000 sztuk jest zgłoszonych w Systemie Informacyjnym Schengen jako skradzione lub zagubione. Rynek szybkich przesyłek i nowe technologie, takie jak drukowanie przestrzenne, sprawiają, że nielegalny handel bronią palną przybiera nowe formy pozwalające uniknąć kontroli. Rosyjska wojna napastnicza przeciwko Ukrainie również zwiększyła ryzyko rozprzestrzeniania broni palnej. W październiku 2022 r. Komisja przyjęła wniosek dotyczący aktualizacji obowiązujących przepisów w sprawie przywozu, wywozu i tranzytu broni palnej do użytku cywilnego, aby zlikwidować luki w obowiązujących przepisach, które mogą zwiększyć liczbę broni palnej przemycanej do UE i takiej, której zastosowanie jest zmieniane po przekroczeniu granic Unii[37]. W perspektywie średnioterminowej nowe przepisy przyczynią się do zmniejszenia ryzyka obchodzenia embarga w przypadku wywozu broni palnej do użytku cywilnego oraz do zwiększenia kontroli przywozu tego rodzaju broni palnej z państw spoza UE. Współprawodawcy nadal muszą przyjąć stanowiska w sprawie tych przepisów, aby osiągnąć porozumienie co do ich przyjęcia jeszcze przed końcem obecnej kadencji Parlamentu.

Handel ludźmi

Handel ludźmi jest jedną z najcięższych form przestępczości zorganizowanej i stanowi poważne naruszenie praw podstawowych. Głównym celem handlu ludźmi w obrębie UE jest wykorzystywanie seksualne i wyzysk pracowników, ale ofiary tego procederu są także wykorzystywane do przymusowego żebractwa i przestępczości oraz do innych celów. W grudniu 2022 r. Komisja zaproponowała zmianę dyrektywy w sprawie zwalczania handlu ludźmi[38] o zaktualizowane przepisy w celu wyeliminowania niedociągnięć w obecnych ramach

[33] Prekursory narkotyków – prawodawstwo UE (zmienione przepisy) (europa.eu)

[34] Rozporządzenie (WE) nr 273/2004 w sprawie prekursorów narkotykowych i rozporządzenie Rady (WE) nr 111/2005 określające zasady nadzorowania handlu prekursorami narkotyków pomiędzy Wspólnotą a państwami trzecimi.

[35] COM(2020) 768.

[36] Działanie 23 Planu działania w zakresie środków odurzających, COM(2020) 606.

[37] COM(2022) 480.

[38] COM(2022) 732.

prawnych. W szczególności zmieniona dyrektywa, po przyjęciu, obejmowałaby swoim zakresem przymusowe małżeństwa i nielegalną adopcję oraz wprowadziłaby wyraźne odniesienie do internetowego wymiaru handlu ludźmi. Ma ona również przewidywać obowiązkowy system kar dla sprawców i formalne ustanowienie krajowych mechanizmów ukierunkowanej pomocy w celu usprawnienia wczesnej identyfikacji ofiar i transgranicznego kierowania pomocy i wsparcia dla ofiar. W zmienionej dyrektywie świadome korzystanie z usług świadczonych przez ofiary handlu ludźmi uznaje się za przestępstwo i wprowadza się obowiązkowe coroczne gromadzenie danych na temat handlu ludźmi, które ma publikować Eurostat. Rada przyjęła podejście ogólne w czerwcu 2023 r., a Parlament Europejski wciąż pracuje nad przyjęciem swojego stanowiska. Konieczne będzie podjęcie szybkich działań w celu osiągnięcia porozumienia przed końcem kadencji Parlamentu.

Przestępstwa przeciwko środowisku

Przestępstwa przeciwko środowisku stały się globalnym zagrożeniem, rosnącym w tempie 5–7 % rocznie. Znaczne zyski, które takie przestępstwa mogą generować, istniejące luki prawne między państwami członkowskimi oraz niskie ryzyko wykrycia sprzyjają przestępczości zorganizowanej. Według Europolu istnieją przesłanki wskazujące, że wpływy z tego typu działań są wykorzystywane do finansowania terroryzmu. W grudniu 2021 r. Komisja przyjęła wniosek w sprawie zastąpienia dyrektywy z 2008 r. w sprawie ochrony środowiska poprzez prawo karne. We wniosku skoncentrowano się na dopracowaniu i aktualizacji definicji kategorii przestępstw przeciwko środowisku oraz określeniu skutecznych, odstraszających i proporcjonalnych rodzajów i poziomów kar dla osób fizycznych i prawnych. Nowe przestępstwa obejmują przestępstwa związane z nielegalnym wylesianiem, naruszenia unijnych przepisów dotyczących chemikaliów, nielegalne wydobycie wód powierzchniowych lub gruntowych oraz nielegalny recykling statków. Wniosek zmierza do znacznego wzmocnienia łańcucha ścigania przestępstw i zacieśnienia współpracy transgranicznej między organami państw członkowskich a agencjami i organami UE. Parlament Europejski i Rada przyjęły swoje stanowiska w sprawie wniosku i są w trakcie negocjacji, które powinny być w stanie zakończyć do końca roku. Wdrożenia wymaga zmieniony Plan działania[39] przeciwko nielegalnemu handlowi dziką fauną i florą w celu dalszego wzmocnienia działań zapobiegawczych i ścigania.

Odzyskiwanie i konfiskata mienia

Kluczowe znaczenie dla zwalczania przestępczości zorganizowanej ma pozbawienie przestępców nielegalnych dochodów. Dlatego oprócz wniosku dotyczącego zapewnienia organom ścigania dostępu do informacji o rachunkach bankowych w całej UE[40] (w sprawie którego osiągnięto porozumienie polityczne w czerwcu 2023 r.) w maju 2022 r. Komisja przedstawiła wniosek w sprawie odzyskiwania i konfiskaty mienia[41], aby zwiększyć zdolności w zakresie śledzenia, identyfikacji, zabezpieczania i konfiskaty mienia oraz zarządzania mieniem. Najważniejsze przepisy zawarte we wniosku odnoszą się do wymogów dotyczących dochodzeń finansowych oraz dodatkowych uprawnień i narzędzi biur ds. odzyskiwania mienia, a także skuteczniejszych środków zabezpieczania i konfiskaty w odniesieniu do szerszego zestawu przestępstw. Jednym z nowych przestępstw, do których środki te mają mieć zastosowanie, jest naruszenie unijnych środków ograniczających. W grudniu 2022 r. Komisja przyjęła odrębny wniosek mający na celu harmonizację prawnokarnych definicji naruszenia unijnych środków ograniczających i kar za takie naruszenia. Skuteczne wdrażanie

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.

i egzekwowanie unijnych środków ograniczających pozostaje jednym z priorytetowych celów Komisji, a usprawnieniu tych działań służą prace grupy zadaniowej „Freeze and Seize" ustanowionej przez Komisję w odpowiedzi na rosyjską wojnę napastniczą przeciwko Ukrainie. W odniesieniu do obu wniosków Parlament Europejski i Rada przyjęły swoje stanowiska w celu osiągnięcia porozumienia do końca tego roku.

Pakiet na rzecz przeciwdziałania praniu pieniędzy

Pranie pieniędzy wiąże się z praktycznie wszystkimi rodzajami działalności przestępczej generującymi dochody z przestępstw w UE[42], a zatem jest kluczowym elementem, na którym należy się skoncentrować w walce z przestępczością w UE. W lipcu 2021 r. Komisja przedstawiła ambitne wnioski mające na celu wzmocnienie środków UE służących zapobieganiu praniu pieniędzy i finansowaniu terroryzmu[43], a także cztery wnioski ustawodawcze mające na celu skuteczniejsze zapobieganie próbom prania dochodów lub finansowania działalności terrorystycznej przez przestępców za pośrednictwem systemu finansowego oraz wykrywania takich prób. W maju 2023 r. współprawodawcy przyjęli jedną z czterech inicjatyw pakietu w celu zapewnienia identyfikowalności transferów kryptoaktywów[44]. Rozporządzenie to będzie obowiązywać od 30 grudnia 2024 r. i od tego czasu wszyscy dostawcy usług w zakresie kryptoaktywów będą musieli gromadzić i przechowywać informacje o inicjatorze i beneficjencie transferów kryptoaktywów. Pozostałe trzy wnioski mają na celu (i) ustanowienie nowego unijnego Urzędu ds. Przeciwdziałania Praniu Pieniędzy w celu zapewnienia spójnego nadzoru o wysokiej jakości na całym rynku wewnętrznym, w tym w odniesieniu do najbardziej ryzykownych podmiotów transgranicznych oraz wspieranie i koordynowanie prac jednostek analityki finansowej, (ii) ustanowienie zharmonizowanych przepisów dla sektora prywatnego, w tym wprowadzenie ogólnounijnego limitu w wysokości 10 000 EUR dla dużych płatności gotówkowych w zamian za usługi i towary, a także (iii) wzmocnienie uprawnień i narzędzi współpracy właściwych organów. Oczekuje się, że pakiet ten znacznie zwiększy zdolność UE do zwalczania prania pieniędzy i ochrony obywateli UE przed terroryzmem i przestępczością zorganizowaną. Te trzy rozpatrywane wnioski są obecnie przedmiotem negocjacji współprawodawców, którzy chcą osiągnąć porozumienie co do ich przyjęcia jeszcze przed końcem obecnej kadencji Parlamentu.

Komisja wzywa Parlament Europejski i Radę do pilnego zakończenia negocjacji międzyinstytucjonalnych, w każdym razie jeszcze przed końcem kadencji obecnego Parlamentu Europejskiego, dotyczących następujących rozpatrywanych dokumentów:

- wniosek dotyczący dyrektywy w sprawie odzyskiwania i konfiskaty mienia;
- wniosek dotyczący dyrektywy w sprawie harmonizacji prawnokarnych definicji naruszenia unijnych środków ograniczających i kar za takie naruszenia;
- wniosek dotyczący dyrektywy w sprawie zwalczania handlu ludźmi;
- wniosek dotyczący dyrektywy w sprawie poprawy ochrony środowiska poprzez prawo karne;
- wniosek dotyczący pakietu na rzecz przeciwdziałania praniu pieniędzy;

[42] Europol, „Enterprising criminals. Europe's fight against the global networks of financial and economic crime" [„Przedsiębiorczy przestępcy. Walka Europy ze światowymi sieciami przestępstw finansowych i gospodarczych"], 2020.

[43] COM(2021) 420.

[44] Rozporządzenie (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849.

- wniosek dotyczący aktualizacji obowiązujących przepisów w sprawie przywozu, wywozu i tranzytu broni palnej do użytku cywilnego.

Komisja wzywa państwa członkowskie, agencje i organy UE do:

- współpracy na rzecz realizacji 17 działań przewidzianych w unijnym planie działania na rzecz zwalczania nielegalnego obrotu środkami odurzającymi i przestępczości zorganizowanej w latach 2023 i 2024.

V. Silny europejski ekosystem bezpieczeństwa

W ostatnich latach zagrożenia bezpieczeństwa mają coraz bardziej transgraniczny charakter, co wymaga dalszych synergii i ściślejszej współpracy na wszystkich szczeblach. Od czasu przyjęcia strategii w zakresie unii bezpieczeństwa podjęto ważne inicjatywy w celu zmaksymalizowania współpracy transgranicznej, usprawnienia i modernizacji dostępnych instrumentów i procedur zarówno na granicach zewnętrznych, jak i w strefie Schengen, a także usprawnienia wymiany informacji między organami ścigania a organami sądowymi w celu lepszego zwalczania przestępczości zorganizowanej. W tym kontekście skuteczne wdrożenie ram interoperacyjności na potrzeby wymiany danych jest ważnym filarem służącym zwiększeniu bezpieczeństwa i skutecznej europejskiej reakcji na zagrożenia transgraniczne, a jednocześnie gwarantuje swobodny przepływ wewnętrzny.

Intensywniejsza wymiana informacji w strefie Schengen: dane pasażera przekazywane przed podróżą (API), dane dotyczące przelotu pasażera (PNR) i Prüm II

Dwa wnioski w sprawie API przyjęte przez Komisję w grudniu 2022 r.[45] mają zwiększyć bezpieczeństwo wewnętrzne Unii przez zapewnienie organom ścigania państw członkowskich dodatkowych narzędzi do zwalczania poważnej przestępczości i terroryzmu. W szczególności dane pasażera przekazywane przed podróżą w przypadku lotów wewnątrzunijnych, wykorzystywane wraz z danymi PNR osób podróżujących drogą powietrzną, mają umożliwić organom ścigania państw członkowskich znaczne zwiększenie skuteczności prowadzonych przez nie dochodzeń dzięki bardziej ukierunkowanym interwencjom. Ważne jest, aby proponowane przepisy zostały przyjęte jak najszybciej: wspomoże to zwalczanie przestępczości zorganizowanej i terroryzmu, jak również znacznie ograniczy potrzebę systematycznych kontroli wszystkich podróżnych w przypadku tymczasowego przywrócenia kontroli na granicach wewnętrznych, a przy tym ułatwi podróże lotnicze i zapewni swobodę przemieszczania się. 6 września 2023 r. Komisja Europejska zaleciła Radzie wyrażenie zgody na negocjacje ze Szwajcarią, Islandią i Norwegią w sprawie umów o przekazywaniu danych PNR. Przyjęcie zaleceń dotyczących tych trzech krajów przyczyniłoby się do zapewnienia spójnej i skutecznej polityki zewnętrznej UE w zakresie danych PNR.

W walce z przestępczością zorganizowaną, narkotykami, terroryzmem, wykorzystywaniem seksualnym i handlem ludźmi policja codziennie korzysta z wymiany na podstawie decyzji Prüm. Wniosek dotyczący rozporządzenia w sprawie zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej („Prüm II")[46] zmienia istniejące ramy z Prüm w celu wyeliminowania luk informacyjnych i usprawnienia zapobiegania przestępstwom, wykrywania

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.

ich i prowadzenia postępowań przygotowawczych w ich sprawie w UE. Zmienione przepisy dotyczące zautomatyzowanej wymiany danych na potrzeby współpracy policyjnej są uzupełnieniem wniosków dotyczących współpracy policyjnej w tym obszarze, a także przyjętych już zaleceń Rady dotyczących wzmocnienia operacyjnej współpracy transgranicznej oraz dyrektywę w sprawie wymiany informacji między organami ścigania. Szybkie przyjęcie i wdrożenie tych powiązanych instrumentów może poprawić, ułatwić i przyspieszyć wymianę danych między organami ścigania oraz pomóc w identyfikacji przestępców.

W pełni interoperacyjny system zarządzania granicami na rzecz bezpiecznej, silnej, cyfrowej i zjednoczonej strefy Schengen

Dobrze funkcjonująca strefa Schengen bez granic wewnętrznych opiera się na wzajemnym zaufaniu między państwami członkowskimi. To z kolei wymaga skutecznych kontroli, czy to na granicach zewnętrznych Unii, czy też w ramach alternatywnych środków na terytorium państw członkowskich. We wniosku Komisji dotyczącym zmiany kodeksu granicznego Schengen[47] określono, jak państwa członkowskie mogą lepiej wykorzystywać rozwiązania alternatywne dla kontroli na granicach wewnętrznych, które mogą zapewnić wysoki poziom bezpieczeństwa. Przyjęcie i pełne wdrożenie zmiany kodeksu granicznego Schengen jest istotne dla zapewnienia wysokiego i proporcjonalnego poziomu bezpieczeństwa w strefie Schengen. Wciąż trwają także prace nad nową architekturą systemów informacyjnych UE w celu lepszego wsparcia pracy organów krajowych z myślą o zapewnieniu bezpieczeństwa oraz zarządzania granicami. Obejmuje ona odnowiony System Informacyjny Schengen, europejski system informacji o podróży oraz zezwoleń na podróż, system wjazdu/wyjazdu, aktualizację wizowego systemu informacyjnego oraz ramy interoperacyjności gwarantujące w pełni bezpieczne połączenie tych systemów. Po całkowitym wdrożeniu ta nowa architektura ma zapewnić organom krajowym bardziej kompleksowe i wiarygodne informacje na temat bezpieczeństwa. Wszystkie elementy ram interoperacyjności mają zasadnicze znaczenie, co oznacza, że opóźnienie w jednym aspekcie lub w jednym państwie członkowskim prowadzi do opóźnienia we wdrażaniu wszystkich aspektów we wszystkich państwach. Opóźnienia w rozwoju technicznym systemu wjazdu/wyjazdu należy ograniczyć do minimum, tak aby system wjazdu/wyjazdu mógł zacząć działać jak najszybciej i aby można było wprowadzić wszystkie kluczowe elementy ram interoperacyjności.

Wniosek w sprawie kontroli przesiewowej[48] ma zwiększyć bezpieczeństwo w strefie Schengen dzięki stworzeniu jednolitych zasad identyfikacji obywateli państw trzecich niespełniających warunków wjazdu, o których mowa w kodeksie granicznym Schengen, oraz poddawania ich kontroli stanu zdrowia i kontroli bezpieczeństwa na granicach zewnętrznych. Wsparciem w realizacji tych celów ma być proponowany system Eurodac, który na podstawie kontroli przesiewowej będzie wskazywać przypadki, w których dana osoba może stanowić zagrożenie dla bezpieczeństwa wewnętrznego. To z kolei ułatwi wdrażanie proponowanego rozporządzenia w sprawie zarządzania azylem i migracją. Komisja zachęca współprawodawców do szybkiego zakończenia negocjacji w sprawie tych przepisów przed końcem obecnej kadencji.

Zwalczanie korupcji

Korupcja ma zdecydowanie szkodliwy wpływ na demokracje, gospodarkę i społeczeństwo, ponieważ działa jako czynnik umożliwiający przestępczość zorganizowaną i wrogie ingerencje zagraniczne. Skuteczne zapobieganie i zwalczanie korupcji ma podstawowe znaczenie

[47] COM(2021) 891.
[48] COM(2020) 612.

w kontekście zarówno ochrony wartości UE, jak i zapewnienia skuteczności polityki UE, utrzymania praworządności i podtrzymania zaufania obywateli do rządzących i do instytucji publicznych. Zgodnie z zapowiedzią przewodniczącej Ursuli von der Leyen zawartą w orędziu o stanie Unii z 2022 r. Komisja przyjęła 3 maja 2023 r. pakiet środków antykorupcyjnych[49]. Wniosek Komisji dotyczący dyrektywy w sprawie zwalczania korupcji obejmuje wzmocnienie przepisów kryminalizujących przestępstwa korupcyjne i ujednolicających kary w całej UE. Umożliwia on także skuteczne prowadzenie postępowań przygotowawczych i ściganie. Kładzie się w nim silny nacisk na działania zapobiegawcze i tworzenie kultury uczciwości, w której nie toleruje się korupcji. W Parlamencie Europejskim i Radzie rozpoczęto już rozmowy na temat tego wniosku. Państwa członkowskie są ponadto proszone o wdrożenie zaleceń wynikających z filaru dotyczącego zwalczania korupcji zawartego w sprawozdaniu na temat praworządności z 2023 r. przyjętym 5 lipca 2023 r. Wniosek wysokiego przedstawiciela, wspierany przez Komisję, zawiera również propozycję ustanowienia specjalnego systemu sankcji w ramach wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) w celu zwalczania poważnych przypadków korupcji na całym świecie.

Wzmocnienie praw ofiar

12 lipca 2023 r. Komisja przedstawiła wniosek dotyczący zmiany dyrektywy o prawach ofiar, aby zapewnić ofiarom większy dostęp do informacji, wsparcia i ochrony, uczestniczenia w postępowaniu karnym oraz dostępu do kompensaty. Jednym z ogólnych celów rewizji jest zapewnianie wysokiego poziomu bezpieczeństwa dzięki stworzeniu bezpieczniejszego środowiska dla ofiar, które będzie zachęcać do zgłaszania przestępstw i pozwoli zmniejszyć obawy przed odwetem.

Komisja wzywa Parlament Europejski i Radę do pilnego zakończenia negocjacji międzyinstytucjonalnych, w każdym razie jeszcze przed końcem kadencji obecnego Parlamentu Europejskiego, dotyczących następujących rozpatrywanych dokumentów:

- wniosek dotyczący rozporządzenia Prüm II;
- wnioski dotyczące danych pasażera przekazywanych przed podróżą (API);
- wnioski dotyczące zwalczania korupcji, a w szczególności w sprawie ustanowienia specjalnego systemu sankcji w ramach wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB);
- wniosek dotyczący rozporządzenia w sprawie zmiany kodeksu granicznego Schengen;
- wniosek dotyczący dyrektywy o prawach ofiar;
- wniosek dotyczący kontroli przesiewowych.

Komisja wzywa państwa członkowskie do:

- zapewnienia jak najszybszego wejścia w życie systemu wjazdu/wyjazdu w celu zakończenia wdrażania unijnej architektury wymiany informacji.

VI. Realizacja

Odpowiedzialność za zapewnienie bezpieczeństwa Europy jako całości jest wspólna i każdy podmiot musi odegrać w tym swoją rolę, począwszy od przyjęcia przez Komisję i współprawodawców nowych, zdecydowanych, kompleksowych i praktycznych przepisów, przez szybką transpozycję oraz szybkie wdrożenie i stosowanie tych przepisów przez państwa

[49] COM(2023) 234.

członkowskie, aż po działania operacyjne prowadzone w terenie przez różne organy, organizacje i zainteresowane strony. Kluczową rolę odgrywają również agencje UE w dziedzinie wymiaru sprawiedliwości, spraw wewnętrznych i cyberbezpieczeństwa, przy czym ich rola zwiększyła się dzięki niedawnemu rozszerzeniu ich obowiązków.

Usprawniona kontrola beneficjentów unijnego finansowania

Podczas wykonywania budżetu UE Komisja odpowiada za dopilnowanie, by beneficjenci finansowania unijnego działali z poszanowaniem wartości UE. Mechanizmy i systemy kontroli określające, kto może korzystać z finansowania unijnego, już teraz są solidne, a trwające negocjacje w sprawie przekształcenia rozporządzenia finansowego mają również na celu zapewnienie Komisji większych środków prawnych do działania w razie potrzeby. Komisja pracuje ponadto nad sposobami dalszego usprawnienia kontroli obecnych i potencjalnych przyszłych beneficjentów finansowania unijnego przez udoskonalenie wytycznych dotyczących obowiązków związanych z poszanowaniem wartości UE oraz konsekwencji, które powinny być następstwem naruszenia wartości Unii. W wytycznych doprecyzowane zostaną obowiązki zarówno beneficjentów, jak i podmiotów przeprowadzających kontrole na szczeblu UE, a sam dokument może służyć jako źródło inspiracji dla organów na szczeblu krajowym. W przypadku naruszenia warunków finansowania Komisja nie zawaha się wstrzymać współpracy z beneficjentami danego projektu i w razie potrzeby zażąda zwrotu środków. Ważne jest, aby państwa członkowskie aktywnie dzieliły się z Komisją zdobytymi informacjami o możliwym ryzyku związanym z organizacjami ubiegającymi się o finansowanie unijne.

Uchybienia zobowiązaniom państwa członkowskiego

W dziedzinie bezpieczeństwa Komisja przeprowadziła wiele postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego. Na przykład w 2023 r. wszczęto dużą liczbę postępowań w sprawie uchybienia zobowiązaniom państwa członkowskiego w związku z niewypełnieniem obowiązków wynikających z rozporządzenia z 2021 r. w sprawie rozpowszechniania w internecie treści o charakterze terrorystycznym (16 państw członkowskich)[50], a w latach 2022–2023 dwadzieścia państw członkowskich otrzymało dodatkowe wezwania do usunięcia uchybienia ze względu na nieprawidłowe wdrożenie dyrektywy z 2011 r. w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych[51]. Nadal otwarta jest znaczna liczba postępowań w sprawie uchybienia zobowiązaniom w związku z niezgodnością przepisów krajowych z dyrektywą w sprawie zwalczania terroryzmu z 2017 r.[52] i w związku z brakiem transpozycji przepisów ułatwiających korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania[53]. Inne obszary, w których toczą się postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, obejmują prawodawstwo dotyczące broni palnej; przepisy dotyczące substancji psychoaktywnych stosowanych w narkotykach, zwalczanie fałszowania i oszustw

[50] Rozporządzenie (UE) 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym.

[51] Dyrektywa (UE) 2011/93 w sprawie zwalczania niegodziwego traktowania dzieci w celach seksualnych.

[52] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW.

[53] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1153 z dnia 20 czerwca 2019 r. ustanawiająca zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania oraz uchylająca decyzję Rady 2000/642/WSiSW.

związanych z bezgotówkowymi środkami płatniczymi, zwalczanie prania pieniędzy, wymianę informacji z rejestrów karnych między państwami członkowskimi UE oraz dyrektywę o prawach ofiar. Państwom członkowskim wdrażającym uzgodnione inicjatywy i działania udostępniono wsparcie (techniczne i finansowe), a Komisja zachowuje gotowość do współpracy z państwami członkowskimi w celu optymalizacji wdrażania.

Monitorowanie za pomocą ocen Schengen i nowego systemu zarządzania

Mechanizm oceny i monitorowania stosowania dorobku Schengen niezmiennie przyczynia się do skutecznego wdrażania przepisów Schengen mających na celu zwiększenie bezpieczeństwa na obszarze bez kontroli na granicach wewnętrznych. W 2023 r. przeprowadzono pierwsze oceny w ramach wzmocnionego mechanizmu oceny i monitorowania stosowania dorobku Schengen, co umożliwiło terminową identyfikację i wyeliminowanie strategicznych słabych punktów, które mają transgraniczny wpływ na bezpieczeństwo i ochronę w UE. Oprócz tego w 2023 r. Komisja rozpoczęła tematyczną ocenę Schengen dotyczącą praktyk państw członkowskich stojących w obliczu podobnych wyzwań w zakresie zwalczania przemytu narkotyków do UE, w szczególności przemytu narkotyków w dużych ilościach. W ocenach tych położono większy i bardziej kompleksowy nacisk na aspekty bezpieczeństwa strefy Schengen. Na podstawie wyników okresowych, tematycznych i niezapowiedzianych ocen Schengen Rada ustanowiła w czerwcu 2023 r. priorytety cyklu Schengen 2023/2024. Określiła obszary priorytetowe wymagające dodatkowych bodźców z myślą o bezpieczniejszej i silniejszej strefie Schengen. Skuteczna i szybka realizacja tych priorytetów oraz wzmożona koordynacja polityki Rady ds. Schengen pozwolą jeszcze bardziej nasilić walkę z przestępczością zorganizowaną i zmaksymalizować transgraniczną współpracę operacyjną.

Rola agencji i organów UE

Zasadnicze znaczenie dla realizacji inicjatyw w zakresie unii bezpieczeństwa ma partnerstwo, ponieważ do osiągnięcia konkretnych rezultatów potrzebne są działania różnych urzędów i organów, zarówno krajowych, jak i europejskich. Na przykład EMPACT (europejska multidyscyplinarna platforma przeciwko zagrożeniom przestępstwami) umożliwia zorganizowaną wielodyscyplinarną współpracę państw członkowskich, wspieraną przez wszystkie instytucje, organy, urzędy i agencje Unii (takie jak Europol, Frontex, Eurojust, CEPOL, OLAF, eu-LISA). Operacje prowadzone przez EMPACT, w tym za pośrednictwem specjalnych operacyjnych grup zadaniowych, służą koordynacji działań państw członkowskich i partnerów operacyjnych w zakresie zwalczania siatek przestępczych i poważnej przestępczości. W samym 2022 r. EMPACT przyczyniła się do łącznie 9 922 aresztowań, zajęcia mienia i pieniędzy o wartości ponad 180 mln EUR, wszczęcia 9 263 dochodzeń, zidentyfikowania 4 019 ofiar, konfiskaty ponad 62 ton narkotyków, zidentyfikowania 51 celów o dużym znaczeniu i aresztowania 12 z nich, a także pozwoliła na przeprowadzenie operacji w kontekście wojny napastniczej przeciwko Ukrainie, w szczególności ukierunkowanych na zwalczanie handlu ludźmi i zagrożeń związanych z bronią palną[54].

Frontex, Europejska Agencja Bezpieczeństwa Morskiego (EMSA) i Europejska Agencja Kontroli Rybołówstwa (EFCA) nadal zacieśniają współpracę w zakresie funkcji straży przybrzeżnej, aby wspierać organy krajowe w zwiększaniu bezpieczeństwa i ochrony na morzu. Agencje te w znacznym stopniu przyczynią się do realizacji strategii Unii Europejskiej w zakresie bezpieczeństwa morskiego.

[54] Zestawienia wyników EMPACT z 2022 r.: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

Szereg inicjatyw w zakresie unii bezpieczeństwa doprowadziło do wprowadzenia nowych obowiązków i zadań dla odpowiednich agencji, co niekiedy miało wpływ na zasoby ludzkie.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Jeżeli chodzi o gotowość i reagowanie na incydenty w celu zwiększenia cyberbezpieczeństwa, Komisja ustanowiła krótkoterminowe działanie wspierające państwa członkowskie i przeniosła środki z programu „Cyfrowa Europa" do **Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)** w celu zwiększenia gotowości i zdolności do reagowania na poważne cyberincydenty. Wynikiem tego działania jest wniosek dotyczący aktu w sprawie cybersolidarności przyjęty w kwietniu 2023 r., a po jego przyjęciu przez współprawodawców ENISA może otrzymać dodatkowe zadania, takie jak obsługa przyszłej unijnej rezerwy na potrzeby cyberbezpieczeństwa i administrowanie nią lub przygotowanie sprawozdania z przeglądu incydentu w następstwie cyberincydentów na dużą skalę. W proponowanym akcie dotyczącym cyberodporności zakłada się powierzenie ENISA zadania przyjmowania od producentów zgłoszeń dotyczących podatności w produktach z elementami cyfrowymi oraz incydentów mających wpływ na bezpieczeństwo tych produktów, które ENISA powinna przekazać odpowiednim CSIRT lub odpowiednim pojedynczym punktom kontaktowym państw członkowskich. Oczekuje się również, że ENISA przygotuje co dwa lata sprawozdanie techniczne na temat pojawiających się tendencji w zakresie ryzyka w cyberprzestrzeni dotyczącego produktów z elementami cyfrowymi oraz przedłoży je grupie współpracy NIS.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) oraz sieć krajowych ośrodków koordynacji to nowe organy Unii, których zadaniem jest wspieranie innowacji i polityki przemysłowej w dziedzinie cyberbezpieczeństwa. Ekosystem ten pomoże wzmocnić zdolności społeczności technologicznych w zakresie cyberbezpieczeństwa, utrzymać doskonałość badawczą i umocnić konkurencyjność przemysłu Unii w tej dziedzinie. ECCC i krajowe ośrodki koordynacji będą podejmować strategiczne decyzje inwestycyjne i łączyć zasoby Unii, jej państw członkowskich i – pośrednio – przemysłu w celu poprawy i wzmocnienia technologicznych i przemysłowych zdolności w zakresie cyberbezpieczeństwa. ECCC ma zatem do odegrania kluczową rolę w realizacji ambitnych celów w zakresie cyberbezpieczeństwa założonych w programie „Cyfrowa Europa" i w programie „Horyzont Europa".

ECCC obsadziło ponad połowę stanowisk swojego personelu, a wkrótce zatrudni dyrektora wykonawczego. Prowadzone już prace obejmują część programu „Cyfrowa Europa" dotyczącą cyberbezpieczeństwa oraz nowy program strategiczny[55] na rzecz rozwoju i wdrażania technologii, w którym określono działania priorytetowe mające na celu wspieranie MŚP w opracowywaniu i wykorzystywaniu strategicznych technologii, usług i procesów w zakresie cyberbezpieczeństwa, wspieranie i rozwój profesjonalnej siły roboczej oraz wzmocnienie wiedzy fachowej w zakresie badań naukowych, rozwoju i innowacji w szerszym europejskim ekosystemie cyberbezpieczeństwa.

Europol

Dzięki nowemu mandatowi **Europol** będzie lepiej przygotowany do wspierania państw członkowskich w zwalczaniu przestępczości zorganizowanej. Jednym z kluczowych priorytetów z uwagi na rosnące znaczenie i coraz większy negatywny wpływ na

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_pl

bezpieczeństwo obywateli UE jest walka z nielegalnym obrotem środkami odurzającymi. W następstwie upoważnienia udzielonego 15 maja 2023 r. przez Radę Unii Europejskiej Komisja aktywnie pracuje nad zawarciem umów międzynarodowych z Boliwią, Brazylią, Ekwadorem, Meksykiem i Peru dotyczących wymiany danych osobowych z Europolem w celu zapobiegania poważnej przestępczości i terroryzmowi oraz ich zwalczania.

Eurojust

Dzięki ponad dwudziestoletniemu doświadczeniu w zapewnianiu organom krajowym wsparcia sądowego w zwalczaniu różnego rodzaju poważnej i złożonej przestępczości transgranicznej **Eurojust** utrwalił swoją pozycję w unijnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Aby zacieśnić współpracę we wszystkich dziedzinach, Komisja negocjuje umowy międzynarodowe w celu ułatwienia współpracy między Eurojustem a 13 państwami trzecimi w zakresie wymiany danych osobowych na potrzeby zwalczania przestępczości zorganizowanej i terroryzmu[56]. Zakończono już negocjacje z Armenią i Libanem, toczą się negocjacje z Algierią i Kolumbią, a także rozpoczęto negocjacje z Bośnią i Hercegowiną. Komisja zachęca Parlament Europejski i Radę do sfinalizowania umów z tymi państwami przed końcem kadencji Parlamentu w celu wzmocnienia transnarodowej współpracy sądowej i poszerzenia zakresu walki z przestępczością transgraniczną.

Prokuratura Europejska

Prokuratura Europejska (EPPO), która rozpoczęła działania operacyjne w czerwcu 2021 r., okazała się potężnym instrumentem w unijnym zestawie narzędzi do prowadzenia postępowań przygotowawczych i oskarżania w sprawach dotyczących przestępstw mających wpływ na budżet Unii, w tym przestępstw związanych z przynależnością do organizacji przestępczej, gdy głównym obszarem działalności są przestępstwa przeciwko budżetowi Unii. Komisja zachęca państwa członkowskie, które nie uczestniczą jeszcze we wzmocnionej współpracy w ramach Prokuratury Europejskiej, by uczyniły to jak najszybciej, co pozwoli w pełni wykorzystać jej potencjał w zakresie ochrony pieniędzy podatników UE.

EUDA

Wraz z nowym mandatem przyjętym przez współprawodawców w czerwcu 2023 r. działające dotychczas Europejskie Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA) przekształci się w pełnoprawną agencję – **Agencję Unii Europejskiej ds. Narkotyków (EUDA)** – o zwiększonej roli. Agencja będzie miała możliwość przeprowadzania bardziej kompleksowej oceny nowych wyzwań w zakresie zdrowia i bezpieczeństwa związanych z niedozwolonymi środkami odurzającymi, a także będzie mogła skuteczniej wnosić wkład w pracę w państwach członkowskich i na szczeblu międzynarodowym. Głównym zadaniem agencji wciąż będzie gromadzenie, analiza i rozpowszechnianie danych, ale rozszerzony mandat umożliwi jej też rozwijanie ogólnych zdolności do oceny zagrożeń zdrowia i bezpieczeństwa w celu identyfikacji pojawiających się zagrożeń, w tym związanych z politoksykomanią, zacieśnienie współpracy za pośrednictwem krajowych punktów kontaktowych oraz utworzenie sieci laboratoriów dostarczających agencji danych kryminalistycznych i toksykologicznych. Ułatwi to agencji wydawanie ostrzeżeń w przypadku pojawienia się na rynku szczególnie niebezpiecznych substancji oraz podnoszenie świadomości społecznej.

[56] Są to Algieria, Argentyna, Armenia, Bośnia i Hercegowina, Brazylia, Kolumbia, Egipt, Izrael, Jordania, Liban, Maroko, Tunezja i Turcja.

Komisja wzywa Parlament Europejski i Radę do pilnego zakończenia negocjacji międzyinstytucjonalnych, w każdym razie jeszcze przed końcem kadencji obecnego Parlamentu Europejskiego, dotyczących następujących rozpatrywanych dokumentów:

- wniosek dotyczący przekształcenia rozporządzenia finansowego.

Komisja wzywa państwa członkowskie do:

- aktywnego dzielenia się z Komisją zdobytymi informacjami o możliwym ryzyku związanym z organizacjami ubiegającymi się o finansowanie unijne;
- szybkiego wdrożenia priorytetów cyklu Schengen 2023/2024 z myślą o bezpieczniejszej i silniejszej strefie Schengen;
- zajęcia się problemami, których dotyczą toczące się przeciwko nim postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, aby zapewnić prawidłową transpozycję odnośnych przepisów.

VII. Wnioski

Ostatnie trzy lata upłynęły pod znakiem nieustannych i zdecydowanych działań w celu urzeczywistnienia ambitnego planu utworzenia unii bezpieczeństwa w UE. W całej dziedzinie polityki bezpieczeństwa poczyniono ogromne postępy. Obecne realia obfitujące w stale zmieniające się zagrożenia wymagają ciągłych starań i nowej motywacji. Prace nad ramami legislacyjnymi należy zakończyć z odpowiednim wyprzedzeniem przed końcem kadencji Parlamentu wiosną 2024 r. Państwa członkowskie mają stałe obowiązki w zakresie transpozycji, wdrażania i stosowania nowych przepisów. Wdrażanie wymaga skoordynowanych działań, również przy wsparciu ze strony agencji UE, a bardzo często także coraz ściślejszej współpracy z naszymi partnerami międzynarodowymi.

Tylko dzięki wspólnym i zdecydowanym działaniom wszystkich zainteresowanych stron możemy osiągnąć taki poziom bezpieczeństwa i ochrony w UE, którego oczekują obywatele, a w obecnej sytuacji wnoszenie wkładu w zwiększanie bezpieczeństwa UE powinno być priorytetem dla każdego.