KOMISJA
EUROPEJSKA

Bruksela, dnia 24.7.2020 r.
COM(2020) 605 final

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

w sprawie strategii UE w zakresie unii bezpieczeństwa

I. Wprowadzenie

W wytycznych politycznych Komisja jednoznacznie stwierdziła, że musimy zrobić wszystko, co w naszej mocy, aby chronić obywateli Unii. Ochrona ta zapewnia nie tylko bezpieczeństwo osobiste, ale również prawa podstawowe, a także buduje fundament zaufania do gospodarki, społeczeństwa i demokracji w UE i ich dynamicznego rozwoju. Europejczycy są dzisiaj świadkami stale zmieniającej się sytuacji w zakresie bezpieczeństwa, na którą wpływ mają ewoluujące zagrożenia, a także inne czynniki, w tym zmiana klimatu, tendencje demograficzne i brak stabilności politycznej poza naszymi granicami. Globalizacja, swobodny przepływ i transformacja cyfrowa nie przestają zapewniać nam dobrobytu, ułatwiają nam życie, a także są motorem innowacji i wzrostu. Przynoszą one też jednak pewne nieodłączne zagrożenia i koszty. Mogą zostać wykorzystane do celów terroryzmu, zorganizowanej przestępczości oraz handlu środkami odurzającymi i ludźmi, a więc działalności, która stanowi bezpośrednie zagrożenie dla obywateli i naszego europejskiego stylu życia. Stale nasilają się cyberprzestępstwa i cyberataki. Poza tym struktura zagrożeń dla bezpieczeństwa staje się coraz bardziej skomplikowana: ataki są ułatwione dzięki możliwości pracy w wymiarze transgranicznym i wzajemnym połączeniom; do powstawania zagrożeń przyczynia się także rozmycie granic między światem fizycznym i cyfrowym; sprawcy wykorzystują grupy podatne na zagrożenia oraz różnice społeczne i gospodarcze. Ataki mogą nastąpić bez żadnego ostrzeżenia, a ich sprawcy pozostawiają po sobie znikome ślady lub nie zostawiają ich wcale. Zarówno podmioty państwowe, jak i niepaństwowe mogą wykorzystywać różnego rodzaju środki stanowiące zagrożenia hybrydowe[1], a to, co wydarza się poza UE, może mieć ogromny wpływ na bezpieczeństwo wewnętrzne UE.

Kryzys związany z COVID-19 zmienił także nasze postrzeganie zagrożeń dla bezpieczeństwa i ochrony oraz odnośnych strategii. Uwydatnił on konieczność zagwarantowania bezpieczeństwa zarówno w środowisku fizycznym, jak i cyfrowym. Sprawił, że zdaliśmy sobie sprawę ze znaczenia otwartej strategicznej autonomii naszych łańcuchów dostaw w odniesieniu do najważniejszych produktów, usług, infrastruktury i technologii. Kryzys sanitarny zwrócił ponadto uwagę na potrzebę włączenia się wszystkich sektorów i obywateli we wspólne działania mające zapewnić, aby UE była przede wszystkim lepiej przygotowana i odporniejsza oraz posiadała lepsze narzędzia pozwalające jej na reagowanie, gdy jest to konieczne.

Obywateli nie można chronić wyłącznie przez działania podejmowane samodzielnie przez poszczególne państwa członkowskie. Nigdy wcześniej poleganie na naszych mocnych stronach w celu współpracy nie było tak ważne i nigdy wcześniej UE nie posiadała tak dużego potencjału pozwalającego jej wprowadzić zmiany. UE może dawać przykład przez udoskonalenie swojego ogólnego systemu zarządzania kryzysowego oraz przez działanie w obrębie swoich granic i poza nimi na rzecz stabilności na świecie. Choć główna odpowiedzialność za bezpieczeństwo spoczywa na państwach członkowskich, ostatnie lata przyniosły większą świadomość faktu, iż bezpieczeństwo każdego pojedynczego państwa członkowskiego jest równoznaczne z bezpieczeństwem wszystkich państw członkowskich. UE może reagować na zagrożenia w multidyscyplinarny i zintegrowany sposób,

[1] Choć nie ma jednej definicji zagrożeń hybrydowych, można je określić jako połączenie działań odwetowych i destabilizujących, metod konwencjonalnych i niekonwencjonalnych (np. dyplomatycznych, wojskowych, gospodarczych i technologicznych), które mogą być stosowane w skoordynowany sposób przez podmioty państwowe lub niepaństwowe, aby osiągnąć konkretne cele (jednak metod tych ani działań nie można jeszcze uznać za oficjalnie wypowiedzianą wojnę). Zob. JOIN(2016) 18 (final).

dostarczając podmiotom odpowiadającym za bezpieczeństwo w państwach członkowskich potrzebne im narzędzia i informacje[2].

UE może również zapewnić, aby polityka bezpieczeństwa pozostała mocno zakorzeniona we wspólnych wartościach europejskich, które budują fundament zaufania do polityk: poszanowaniu praworządności i jej utrzymaniu, równości[3] i prawach podstawowych oraz zagwarantowaniu przejrzystości, rozliczalności i kontroli demokratycznej. UE może stworzyć rzeczywistą i skuteczną unię bezpieczeństwa, w której prawa i wolności obywateli są dobrze chronione. Bezpieczeństwo i poszanowanie praw podstawowych nie są z sobą sprzeczne: cele te są spójne i uzupełniają się nawzajem. U podstawy polityk w zakresie bezpieczeństwa powinny leżeć nasze wartości i prawa podstawowe. Polityki te powinny gwarantować zasady konieczności, proporcjonalności i legalności, a także obejmować odpowiednie zabezpieczenia w celu zapewnienia rozliczalności i dochodzenia roszczeń na drodze sądowej oraz umożliwiać skuteczne reagowanie w celu ochrony obywateli, zwłaszcza tych najbardziej podatnych na zagrożenia.

Wprowadzono już ważne narzędzia prawne, praktyczne i wspierające, ale trzeba je wzmocnić i lepiej wdrożyć. Dokonano znacznych postępów w usprawnianiu wymiany informacji z państwami członkowskich i współpracy wywiadów oraz w ograniczaniu pola działania terrorystów i przestępców. Nadal utrzymuje się jednak rozproszenie działań.

Zasięg wysiłków UE musi wykraczać poza jej granice. Ochrona Unii i jej obywateli nie sprowadza się już wyłącznie do zapewnienia bezpieczeństwa w granicach UE, ale obejmuje też zewnętrzny wymiar bezpieczeństwa. Istotnym elementem działań UE zmierzających do poprawy bezpieczeństwa na swoim terytorium pozostanie podejście UE do bezpieczeństwa zewnętrznego w ramach wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) oraz wspólnej polityki bezpieczeństwa i obrony (WPBiO). Zasadnicze znaczenie dla skutecznej i wszechstronnej reakcji ma stawienie czoła wspólnym wyzwaniom przez współpracę z państwami trzecimi i na szczeblu globalnym. Stabilność i bezpieczeństwo w sąsiedztwie UE wpływają w dużym stopniu na jej własne bezpieczeństwo.

Nowa strategia, opierająca się na wcześniejszych pracach Parlamentu Europejskiego[4], Rady[5] i Komisji[6], pokazuje, że rzeczywista i skuteczna unia bezpieczeństwa wymaga solidnej bazy w postaci instrumentów i polityk, aby móc realnie zapewniać bezpieczeństwo. Uznano w niej też fakt, że aspekt bezpieczeństwa ma wpływ na wszystkie warstwy społeczeństwa i wszystkie polityki publiczne. UE musi zapewnić bezpieczne środowisko wszystkim obywatelom, niezależnie od ich pochodzenia rasowego lub etnicznego, wyznania, wierzeń, płci, wieku lub orientacji seksualnej.

---

[2] Na przykład poprzez usługi zapewniane przez unijny program kosmiczny taki jak Copernicus, który dostarcza danych z obserwacji Ziemi i ma zastosowanie na potrzeby ochrony granicy, bezpieczeństwa morskiego, ścigania przestępstw, zwalczania aktów piractwa, prewencji w zakresie przemytu środków odurzających oraz zarządzania sytuacjami wyjątkowymi.

[3] Unia równości: strategia na rzecz równouprawnienia płci na lata 2020–2025, COM(2020) 152.

[4] Na przykład prace komisji TERR działającej przy Parlamencie Europejskim, która złożyła sprawozdanie w listopadzie 2018 r.

[5] Od konkluzji Rady z czerwca 2015 r. w sprawie „odnowionej strategii bezpieczeństwa wewnętrznego” po niedawne wyniki posiedzenia Rady w grudniu 2019 r.

[6] „Realizacja Europejskiej agendy bezpieczeństwa w celu zwalczania terroryzmu i utorowania drogi ku rzeczywistej i skutecznej unii bezpieczeństwa”, COM(2016) 230 final, 20.4.2016 r. Zob. niedawna ocena wdrożenia ustawodawstwa w obszarze bezpieczeństwa wewnętrznego pt. „Wdrożenie ustawodawstwa dotyczącego spraw wewnętrznych w obszarze bezpieczeństwa wewnętrznego: 2017–2020” (SWD(2020) 135).

Niniejsza strategia obejmuje lata 2020–2025 i koncentruje się na budowaniu potencjału i zdolności pozwalających zapewnić środowisko bezpieczeństwa, które wytrzyma próbę czasu. Określono w niej obejmujące całe społeczeństwo podejście do bezpieczeństwa, które pozwoli w sposób efektywny i skoordynowany reagować na szybko zmieniający się krajobraz zagrożeń. W strategii wyznaczono również strategiczne priorytety i związane z nimi działania, aby w zintegrowany sposób zaradzić zagrożeniom cyfrowym i fizycznym w całym ekosystemie unii bezpieczeństwa, kładąc nacisk na obszary, w których UE może wnieść dodatkową wartość. Celem strategii jest zaproponowanie korzyści wypływających z bezpieczeństwa, aby chronić wszystkich obywateli w UE.

II. Szybko zmieniający się krajobraz zagrożeń dla bezpieczeństwa w Europie

Bezpieczeństwo, dobrobyt i dobrostan obywateli zależą od tego, czy czują się oni pewnie. Zagrożenia dla tego poczucia pewności zależą z kolei od tego, w jakim stopniu ich życie i źródła utrzymania są podatne na zagrożenia. Im większa podatność na zagrożenia, tym większa jest groźba wykorzystania tej podatności. Zarówno podatność na zagrożenia, jak i same zagrożenia nieustannie ewoluują i UE musi się przystosować do tej sytuacji.

W życiu codziennym polegamy na wielu różnych usługach takich jak dostawa energii, usługi transportowe, finansowe i zdrowotne. Usługi te wymagają zarówno infrastruktury fizycznej, jak i cyfrowej, co zwiększa podatność na zagrożenia i możliwość zakłóceń w ich świadczeniu. Wiele przedsiębiorstw i służb użyteczności publicznej było w stanie utrzymać swoją działalność podczas pandemii COVID-19 tylko dzięki nowym technologiom, które pracę zdalną i utrzymanie logistyki łańcuchów dostaw. Ale technologie te otworzyły jednocześnie furtkę dla złośliwych ataków, których liczba przyrasta w wyjątkowym tempie. Przestępcy usiłują wykorzystać zakłócenia wywołane pandemią i przestawieniem się na pracę zdalną z domu[7]. Niedobory towarów stworzyły nowe możliwości dla przestępczości zorganizowanej. Konsekwencje mogły być śmiertelne: zakłócenia w świadczeniu podstawowych usług zdrowotnych w momencie największej presji.

Fakt, że w naszym życiu na coraz więcej różnych sposobów czerpiemy korzyści z technologii cyfrowych, sprawił, że **cyberbezpieczeństwo** technologii stało się kwestią o strategicznym znaczeniu[8]. Nasze domy, banki, usługi finansowe i przedsiębiorstwa (zwłaszcza te małe i średnie) są poważnie narażone na cyberataki. Współzależność systemów fizycznych i cyfrowych może spotęgować szkody: wszelkie oddziaływanie na systemy fizyczne nieuchronnie wpływa na systemy cyfrowe, a cyberataki na systemy informatyczne i infrastrukturę cyfrową mogą spowodować wstrzymanie świadczenia usług podstawowych[9]. Rosnąca popularność internetu rzeczy i coraz powszechniejsze

[7] Europol „Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU" [„Przyszłość po pandemii. Jak COVID-19 wpłynie na poważną i zorganizowaną przestępczość w UE"] (kwiecień 2020 r.).

[8] Zalecenie Komisji w sprawie cyberbezpieczeństwa sieci 5G, C(2019) 2335; komunikat pt. „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi", COM(2020) 50.

[9] W marcu 2020 r. szpital uniwersytecki w Brnie (Czechy) padł ofiarą cyberataku, który zaburzył przyjmowanie pacjentów i planowane operacje (Europol „Pandemic Profiteering. How criminals exploit the COVID-19 crisis" [„Spekulacje na pandemii. Jak przestępcy wykorzystują kryzys COVID-19"]). Sztuczna inteligencja może być wykorzystywana do ataków cyfrowych, politycznych i fizycznych, a także do prowadzenia obserwacji. Gromadzenie danych w ramach internetu rzeczy (inteligentne zegarki, wirtualni asystenci itp.) może służyć do inwigilacji obywateli.

wykorzystanie sztucznej inteligencji przyniosą wprawdzie nowe korzyści, ale stworzą też nowe zagrożenia.

Nasz świat funkcjonuje w oparciu o infrastrukturę cyfrową, technologie cyfrowe i systemy online, które pozwalają nam prowadzić działalność gospodarczą oraz korzystać z produktów i usług. Komunikowanie się i interakcje są dla nas nieodzowne. To poleganie na internecie utorowało drogę fali **cyberprzestępczości**[10]. Pojawienie się „modelu biznesowego" cyberprzestępczości jako usługi (ang. *cybercrime-as-a-service*) i czarnego rynku cyberprzestępczego sprawia, że produkty i usługi cyberprzestępczości można łatwo znaleźć w internecie. Przestępcy szybko reagują na nowe technologie, wykorzystując je do własnych celów. Na przykład podrobione i sfałszowane produkty lecznicze przedostają się do legalnego łańcucha dostaw produktów farmaceutycznych[11]. Wykładniczy wzrost treści pornograficznych z udziałem małoletniego w internecie[12] ukazuje konsekwencje społeczne zmieniających się modeli przestępczości. Według niedawno przeprowadzonego badania większość mieszkańców UE (55 %) obawia się, że przestępcy i oszuści mogą uzyskać dostęp do ich danych[13].

W otoczeniu globalnym również zwraca się uwagę na te zagrożenia. Asertywne polityki przemysłowe państw trzecich i proceder kradzieży własności intelektualnej wykorzystujący cyberprzestrzeń zmieniają strategiczny paradygmat ochrony i promocji interesów europejskich. Problem ten nasila się w kontekście rozwoju podwójnych zastosowań: silny sektor technologii cywilnych stanowi zatem duży atut z punktu widzenia zdolności obronnych i bezpieczeństwa. Szpiegostwo przemysłowe ma znaczny wpływ na gospodarkę, miejsca pracy i wzrost gospodarczy w UE: koszty cyberkradzieży tajemnic handlowych szacuje się na 60 mld EUR[14]. Sytuacja ta wymaga dogłębnej refleksji nad tym, w jaki sposób zależności i większe narażenie na cyberzagrożenia zmniejsza zdolność UE do ochrony jej obywateli i przedsiębiorstw.

Kryzys związany z COVID-19 uwidocznił również, że podziały społeczne i prekaryjność są źródłem podatności na zagrożenia dla bezpieczeństwa. Rośnie przez to ryzyko bardziej wyrafinowanych i **hybrydowych ataków** podmiotów państwowych i niepaństwowych wykorzystujących słabe punkty. Sprawcy posługują się kombinacją cyberataków, niszczenia infrastruktury krytycznej[15], kampanii dezinformacyjnych i radykalizacji postaw w ramach narracji politycznej.[16]

---

[10] Według niektórych prognoz koszt naruszeń ochrony danych będzie wynosić do 2024 r. 5 bln USD rocznie, co stanowi wzrost z 3 bln USD w 2015 r. (Juniper Research, „The Future of Cybercrime & Security" [„Przyszłość cyberprzestępczości i bezpieczeństwa"]).

[11] W badaniu z 2016 r. (Legiscript) oszacowano, że na całym świecie tylko 4 % aptek internetowych działa zgodnie z prawem, a klienci z UE są grupą docelową dla 30 000–35 000 nielegalnych aptek internetowych.

[12] Strategia UE na rzecz skuteczniejszej walki z niegodziwym traktowaniem dzieci w celach seksualnych, COM(2020) 607.

[13] Agencja Praw Podstawowych Unii Europejskiej, „Your rights matter: Security concerns and experiences, Fundamental Rights Survey" [„Twoje prawa mają znaczenie: obawy dotyczące bezpieczeństwa i doświadczenia w tym zakresie. Badanie dotyczące praw podstawowych"] (2020 r.), Luksemburg, Urząd Publikacji Unii Europejskiej.

[14] „The scale and impact of industrial espionage and theft of trade secrets through cyber" [„Skala i wpływ szpiegostwa przemysłowego i kradzieży tajemnic handlowych w cyberprzestrzeni"] (2018 r.).

[15] Infrastruktura krytyczna ma podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego, a jej zakłócenie lub zniszczenie wywiera istotne skutki (dyrektywa Rady 2008/114/WE).

[16] 97 % obywateli UE styka się z fałszywymi informacjami, w tym 38 % każdego dnia. Zob. JOIN/2020/8 (final).

Zmienia się charakter również tych zagrożeń, z którymi mieliśmy do czynienia już od długiego czasu. W 2019 r. w UE odnotowano tendencję spadkową, jeśli chodzi o **ataki terrorystyczne**. Wciąż duże zagrożenie dla obywateli UE stanowią jednak ataki dżihadystów organizowane z inicjatywy lub inspiracji Daisz i Al-Kaidy oraz powiązanych z nimi grup[17]. Równocześnie wzrasta również zagrożenie ze strony brutalnego ekstremizmu prawicowego[18]. Powodem do poważnych obaw są ataki o podłożu rasistowskim: antysemickie ataki terrorystyczne w Halle, które pociągnęły za sobą ofiary śmiertelne, przypomniały o potrzebie wzmożenia reakcji zgodnie z deklaracją Rady z 2018 r.[19] Jedna na pięć osób w UE poważnie obawia się, że w ciągu najbliższych 12 miesięcy może nastąpić atak terrorystyczny[20]. Zdecydowaną większość niedawnych ataków terrorystycznych stanowiły ataki przy zastosowaniu niezaawansowanej technologii, skierowane przez pojedynczych sprawców przeciwko osobom fizycznym w przestrzeni publicznej. Propaganda terrorystyczna w internecie nabrała nowego znaczenia za sprawą transmisji strumieniowej na żywo ataków w Christchurch[21]. Zagrożenie ze strony osób o radykalnych poglądach pozostaje duże; może je jeszcze zwiększyć powrót zagranicznych bojowników terrorystycznych i ekstremistów wypuszczonych z więzienia[22].

Kryzys unaocznił również, że znane od dawna zagrożenia mogą ewoluować w zmienionej rzeczywistości. Grupy prowadzące **przestępczość zorganizowaną** wykorzystują niedobory towarów jako okazję do otwarcia nowych czarnych rynków. Handel nielegalnymi środkami odurzającymi pozostaje największym rynkiem przestępczym w Unii, a jego wartość detaliczna w UE szacowana jest na co najmniej 30 mld EUR rocznie[23]. Wciąż prowadzi się handel ludźmi: szacuje się, że w skali całego świata roczne dochody z wszystkich form wyzysku ludzi sięgają 30 mld EUR[24]. Międzynarodowy handel podrobionymi produktami leczniczymi osiągnął wartość 38,9 mld EUR[25]. Równocześnie niskie wskaźniki konfiskaty pozwalają przestępcom na dalszą ekspansję ich działalności i przenikanie do legalnej gospodarki[26]. Przestępcy i terroryści mają coraz łatwiejszy dostęp do broni palnej: mogą je kupić na rynku internetowym albo wyprodukować dzięki nowym technologiom takim jak

[17] 13 państw członkowskich UE odnotowało łącznie 119 ataków terrorystycznych (przeprowadzonych zgodnie z planem, nieudanych i udaremnionych), w których zginęło dziesięć osób, a 27 odniosło obrażenia (Europol „European Union Terrorism Situation and Trend Report" [„Sprawozdanie dotyczące sytuacji i trendów w zakresie terroryzmu w Unii Europejskiej"] (2020 r.)).

[18] W 2019 r. doszło do sześciu skrajnie prawicowych ataków terrorystycznych (jeden przeprowadzony zgodnie z planem, jeden nieudany, cztery udaremnione) w trzech państwach członkowskich, w porównaniu z tylko jednym atakiem w 2018 r. Ofiary śmiertelne pociągnęły za sobą także ataki niezaklasyfikowane jako terrorystyczne (Europol, 2020 r.).

[19] Zob. także deklaracja Rady w sprawie zwalczania antysemityzmu i wypracowania wspólnego podejścia do bezpieczeństwa z myślą o skuteczniejszej ochronie społeczności i instytucji żydowskich w Europie.

[20] Agencja Praw Podstawowych Unii Europejskiej „Your rights matter: Security concerns and experiences" (2020 r.).

[21] Od lipca 2015 r. do końca 2019 r. Europol wykrył treści o charakterze terrorystycznym na 361 platformach (Europol, 2020 r.).

[22] Europol „A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism" [„Przegląd transatlantyckich najlepszych praktyk przeciwdziałania radykalizacji postaw w więzieniach i recydywie terrorystów"] (2019 r.).

[23] „EMCDDA and Europol EU Drugs Market Report" [„Sprawozdanie EMCDDA i Europolu na temat rynku środków odurzających w UE"] (2019 r.).

[24] Europol „Report on Trafficking in Human Beings, Financial Business Model" [„Sprawozdanie na temat handlu ludźmi. Finansowy model biznesowy"] (2015 r.).

[25] Urząd Unii Europejskiej ds. Własności Intelektualnej i OECD, sprawozdanie pt. „Trade in counterfeit pharmaceutical products" [„Handel podrobionymi produktami leczniczymi"].

[26] Sprawozdanie pt. „Odzyskiwanie i konfiskata mienia: Przestępstwa nigdy nie mogą się opłacać", COM(2020) 217.

drukowanie przestrzenne[27]. Wraz z rozpowszechnianiem się sztucznej inteligencji, nowych technologii i robotyki będzie się nasilać ryzyko wykorzystywania tych innowacji do celów przestępczych[28].

Zagrożenia te mają przekrojowy charakter i uderzają w różny sposób w poszczególne warstwy społeczne. Wszystkie z nich stanowią poważne zagrożenie dla osób fizycznych i przedsiębiorstw oraz wymagają kompleksowej i spójnej reakcji na poziomie UE. Gdy źródłem zagrożenia dla bezpieczeństwa może być nawet sprzęt AGD, np. podłączone do internetu lodówka czy ekspres do kawy, nie możemy już polegać tylko na służbach państwowych, aby zapewnić sobie bezpieczeństwo. Podmioty gospodarcze muszą wziąć większą odpowiedzialność za cyberbezpieczeństwo produktów i usług, które oferują na rynku; także osoby fizyczne powinny orientować się, przynajmniej w podstawowym stopniu, czym jest cyberbezpieczeństwo, aby móc siebie chronić.

III. Skoordynowana reakcja UE służąca całemu społeczeństwu

UE już pokazała, że potrafi wnieść realną wartość dodaną. Od 2015 r. unia bezpieczeństwa wniosła nowe powiązania, jeśli chodzi o sposób, w jaki na szczeblu UE uwzględniane są strategie bezpieczeństwa. Trzeba jednak uczynić więcej, aby zaangażować całe społeczeństwo, w tym wszystkie szczeble administracji rządowej, przedsiębiorstwa ze wszystkich sektorów gospodarki i obywateli wszystkich państw członkowskich. Rośnie świadomość zagrożeń wynikających z relacji zależności[29] i potrzeba solidnej europejskiej strategii przemysłowej[30]: UE powinna dysponować masą krytyczną w zakresie przemysłu i wytwarzania technologii oraz odpornym łańcuchem dostaw. Siła oznacza również pełne poszanowanie praw podstawowych i wartości UE: są one warunkiem wstępnym prawnie uzasadnionych, skutecznych i wyważonych strategii bezpieczeństwa. Niniejsza strategia unii bezpieczeństwa zakłada konkretne obszary działań w przyszłości. Opracowana została z myślą o następujących wspólnych celach:

- ***Budowanie potencjału i zdolności w zakresie wczesnego wykrywania, zapobiegania i szybkiego reagowania na kryzysy:*** Europa musi zwiększyć swoją odporność, aby zapobiegać przyszłym wstrząsom, chronić się przed nimi i przetrwać je. Musimy zbudować potencjał i zdolności w zakresie wczesnego wykrywania i szybkiego reagowania na kryzysy w obszarze bezpieczeństwa, stosując zintegrowane i skoordynowane podejście, zarówno w drodze światowych inicjatyw, jak i inicjatyw sektorowych (np. w sektorze finansowym, energetycznym, sektorze wymiaru sprawiedliwości, ścigania przestępstw, opieki zdrowotnej, sektorze morskim, sektorze transportu), opierając się na istniejących narzędziach i inicjatywach[31]. Komisja

[27] W 2017 r. w 41 % wszystkich ataków terrorystycznych użyto broni palnej (Europol, 2018 r.).

[28] W lipcu 2020 r. organy ścigania i organy wymiaru sprawiedliwości we Francji i Holandii przeprowadziły wspólnie z Europolem i Eurojustem dochodzenie mające na celu rozbicie EncroChat, zaszyfrowanej sieci telefonicznej używanej przez siatki przestępcze do przeprowadzania brutalnych ataków, korupcji, usiłowań zabójstwa i transportu dużych ilości środków odurzających.

[29] Zależność od zagranicznych podmiotów prowadzi do większego narażenia na ryzyko, np. wykorzystania słabych punktów systemów informatycznych do ataków na infrastrukturę krytyczną (energetyczną, transportową, bankową, systemów zdrowia itp.), przejęcia kontroli nad systemami używanymi do kontroli procesów przemysłowych lub ułatwienia kradzieży danych i szpiegostwa.

[30] Komunikat Komisji pt. „Nowa strategia przemysłowa dla Europy", COM(2020) 102.

[31] Takie jak zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), Centrum Koordynacji Reagowania Kryzysowego, zalecenie Komisji w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (C(2017) 6100), unijny

przedstawi również propozycje dotyczące szeroko zakrojonego systemu zarządzania kryzysowego wewnątrz UE, który może mieć znaczenie również dla kwestii bezpieczeństwa.

- ***Koncentracja na wynikach***: Strategię opartą na wynikach należy opracować na podstawie dokładnej oceny zagrożeń i ryzyka, aby nasze wysiłki były jak najlepiej ukierunkowane. Musi ona określać i stosować słuszne zasady i odpowiednie narzędzia. Potrzebne są wiarygodne strategiczne dane wywiadowcze, które posłużą za podstawę strategii bezpieczeństwa UE. Gdy konieczne jest wprowadzenie prawodawstwa UE, należy kontrolować jego pełne wdrożenie, aby uniknąć fragmentacji i luk, które dawałyby możliwości nadużyć. Skuteczne wprowadzenie w życie niniejszej strategii będzie zależało również od zapewnienia odpowiedniego finansowania w następnym okresie programowania 2021–2027, w tym dla odnośnych agencji UE.
- ***Współdziałanie wszystkich podmiotów w sektorze publicznym i prywatnym:*** Zarówno w sektorze publicznym, jak i prywatnym główni gracze niechętnie dzielą się informacjami dotyczącymi bezpieczeństwa, albo z obawy o naruszenie bezpieczeństwa narodowego albo kierując się względami konkurencyjności.[32] Największą skuteczność działania zapewnia jednak współpraca. W pierwszej kolejności oznacza to intensywniejszą współpracę między państwami członkowskimi, w tym między organami ścigania, organami wymiaru sprawiedliwości i innymi organami publicznymi, a także współpracę z instytucjami i agencjami Unii w celu budowy porozumienia i komunikacji, co jest niezbędne do wypracowania wspólnych rozwiązań. Współpraca z sektorem prywatnym ma kluczowe znaczenie również z tego względu, że sektor przemysłowy jest właścicielem dużej części cyfrowej i niecyfrowej infrastruktury, która jest niezbędna do skutecznego zwalczania przestępczości i terroryzmu. Swój wkład mogą wnieść także osoby fizyczne, na przykład poprzez nabycie umiejętności i wiedzy potrzebnych do zwalczania cyberprzestępczości i dezinformacji. Zasięg opisanych wspólnych wysiłków musi wykraczać poza granice UE. Trzeba budować bliższe relacje z podobnie myślącymi partnerami.

IV. Ochrona wszystkich obywateli w UE: strategiczne priorytety dla unii bezpieczeństwa

UE jest wyjątkowo predysponowana do reagowania na te nowe globalne zagrożenia i wyzwania. Powyższa analiza zagrożeń wskazuje na cztery wzajemnie powiązane strategiczne priorytety, jakimi należy się zająć w przyszłości na poziomie UE, przy pełnym poszanowaniu praw podstawowych: (i) środowisko bezpieczeństwa, które wytrzyma próbę czasu, (ii) zajmowanie się ewoluującymi zagrożeniami, (iii) ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną, (iv) silny europejski ekosystem bezpieczeństwa.

1. Środowisko bezpieczeństwa, które wytrzyma próbę czasu

Ochrona infrastruktury krytycznej i jej odporność

protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym (unijny podręcznik taktyczny), SWD(2016) 227.

[32] Wspólny komunikat pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej”, JOIN(2017) 450.

W życiu codziennym osoby fizyczne zależne są od kluczowej infrastruktury, gdy podróżują, pracują, korzystają z podstawowych usług publicznych, takich jak leczenie szpitalne, transport, dostawy energii, lub gdy korzystają ze swoich demokratycznych praw. Jeśli takiej infrastrukturze brakuje odpowiedniej ochrony lub odporności, ataki mogą spowodować ogromne zakłócenia – w świecie fizycznym bądź w internecie – w poszczególnych państwach członkowskich, a potencjalnie w całej UE.

Obecne ramy unijne dotyczące ochrony i odporności infrastruktury krytycznej[33] nie nadążają za ewoluującymi zagrożeniami. Coraz większe współzależności oznaczają, że zakłócenia w jednym sektorze mogą natychmiast oddziaływać na funkcjonowanie innych sektorów: atak na producentów energii elektrycznej może sparaliżować telekomunikację, szpitale, banki lub porty lotnicze, natomiast atak na infrastrukturę cyfrową może wywołać zakłócenia w sieciach elektroenergetycznych lub systemach finansowych. W miarę jak coraz większa część naszego życia gospodarczego i społecznego przenosi się do internetu, zagrożenia te stają się coraz bardziej poważne. Ramy legislacyjne muszą uwzględniać te rosnące wzajemne powiązania i współzależności przez wprowadzenie solidnych środków, zarówno cyfrowych, jak i fizycznych, w celu ochrony infrastruktury krytycznej i zwiększenia jej odporności. Usługi podstawowe, w tym te opierające się na infrastrukturze kosmicznej, muszą być należycie chronione przed obecnymi i przyszłymi zagrożeniami, ale muszą być również odporne. W tym celu system powinien być zdolny do przygotowania się i opracowania planów na wypadek niekorzystnych zdarzeń, „amortyzowania" takich zdarzeń, odbudowy po ich zajściu i lepszym dostosowaniu się do nich.

Jednocześnie państwa członkowskie korzystają z przysługującego im marginesu swobody i wdrażają istniejące prawodawstwo w różny sposób. Wynikająca stąd fragmentacja może osłabić rynek wewnętrzny i utrudnić koordynację transgraniczną, przede wszystkim w regionach przygranicznych. Operatorzy świadczący usługi podstawowe w różnych państwach członkowskich muszą przestrzegać różnych wymogów sprawozdawczości. Komisja bada, czy **nowe ramy dotyczące infrastruktury fizycznej i cyfrowej** mogą ujednolicić podejście w zakresie niezawodnego zapewniania usług podstawowych. Oprócz takich ram należy przewidzieć **inicjatywy sektorowe**, aby zaradzić konkretnym zagrożeniom dla infrastruktury krytycznej, m.in. w sektorach transportu, przestrzeni kosmicznej, energii, finansów i ochrony zdrowia[34]. Z uwagi na dużą zależność sektora finansowego od usług IT i jego znaczną podatność na cyberataki, w pierwszej kolejności podjęta zostanie inicjatywa dotycząca operacyjnej odporności cyfrowej właśnie w tym sektorze. W związku ze szczególną wrażliwością i znaczeniem systemu energetycznego podjęta zostanie specjalna inicjatywa mająca służyć większej odporności krytycznej infrastruktury energetycznej na zagrożenia fizyczne, cybernetyczne i hybrydowe i zapewnieniu równych warunków działania operatorom systemów energetycznych w innych państwach.

Istotne z punktu widzenia bezpieczeństwa skutki bezpośrednich inwestycji zagranicznych, które to skutki mogą mieć wpływ na infrastrukturę krytyczną lub technologie krytyczne, będą również przedmiotem ocen państw członkowskich UE i Komisji przeprowadzanych

[33] Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. L 194 z 19.7.2016; Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

[34] Z uwagi na przeciążenie sektora opieki zdrowotnej, szczególnie podczas kryzysu wywołanego pandemią COVID-19, Komisja rozważy również inicjatywy mające wzmocnić ramy bezpieczeństwa zdrowotnego w UE, a odpowiedzialne agencje UE będą reagować na poważne transgraniczne zagrożenia zdrowia.

zgodnie z nowymi europejskimi ramami monitorowania bezpośrednich inwestycji zagranicznych[35].

UE może również stworzyć nowe narzędzia, aby zwiększyć odporność infrastruktury krytycznej. Globalny internet wykazywał dotychczas wysoką odporność, zwłaszcza jeśli chodzi o zdolność radzenia sobie z większym wolumenem ruchu. Musimy jednak być przygotowani na ewentualne przyszłe kryzysy zagrażające bezpieczeństwu, stabilności i odporności internetu. Dalsze działanie internetu zostanie zapewnione, jeżeli stanie się on odporny na cyberincydenty i szkodliwe działania w cyberprzestrzeni oraz mniej zależny od infrastruktury i usług znajdujących się poza Europą. Będzie to wymagało połączenia następujących środków: prawodawstwa, w tym przeglądu obecnych przepisów w celu zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i informacji w UE; zwiększonych inwestycji w badania i innowacje; i rozważenia rozmieszczenia lub wzmocnienia w UE podstawowych infrastruktur i zasobów internetowych, zwłaszcza systemu nazw domen[36].

Kluczowe znaczenie dla ochrony najważniejszych unijnych i krajowych aktywów cyfrowych ma stworzenie kanału bezpiecznej komunikacji na potrzeby infrastruktury krytycznej. Komisja pracuje z państwami członkowskimi nad wprowadzeniem certyfikowanej bezpiecznej infrastruktury kwantowej typu „end-to-end", naziemnej i kosmicznej, w połączeniu z bezpiecznym systemem rządowej łączności satelitarnej, o którym jest mowa w rozporządzeniu w sprawie programu kosmicznego[37].

Cyberbezpieczeństwo

Liczba cyberataków dalej rośnie[38]. Ataki te są bardziej wyrafinowane niż kiedykolwiek wcześniej, pochodzą z wielu różnych źródeł w UE i poza jej granicami, a ich celem są obszary o największej podatności na zagrożenia. Agresorami są często państwa lub podmioty wspierane przez państwa, a przedmiotem ataku – kluczowe infrastruktury cyfrowe, takie jak główni dostawcy usług w chmurze[39]. Cyberryzyko stało się poważnym zagrożeniem także dla systemu finansowego. Międzynarodowy Fundusz Walutowy szacuje, że wskutek ataków cybernetycznych banki na całym świecie tracą każdego roku 9 % dochodów netto, czyli ok. 100 mld USD[40]. Przejście na urządzenia podłączone do internetu przyniesie ogromne korzyści użytkownikom, ale w miarę jak coraz mniej danych będzie przechowywanych i przetwarzanych w centrach danych, a coraz więcej – bliżej

---

[35] Od momentu pełnego wejścia w życie w dniu 11 października 2020 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/452 z dnia 19 marca 2019 r. ustanawiającego ramy monitorowania bezpośrednich inwestycji zagranicznych w Unii, UE będzie dysponowała nowym mechanizmem współpracy w zakresie bezpośrednich inwestycji na zewnątrz UE, które mogą wpływać na bezpieczeństwo lub porządek publiczny. Rozporządzenie to przewiduje, że państwa członkowskie i Komisja będą oceniać potencjalne ryzyko związane z takimi bezpośrednimi inwestycjami zagranicznymi i – w stosownych przypadkach oraz gdy zagrożenia dotyczą więcej niż jednego państwa członkowskiego – zaproponują odpowiednie środki ograniczające to ryzyko.

[36] System nazw domen (DNS) jest hierarchicznym i zdecentralizowanym systemem na potrzeby nazywania komputerów, usług lub innych zasobów związanych z internetem lub prywatną siecią. System przekłada nazwy domen na adresy IP potrzebne do lokalizowania i rozpoznawania usług i urządzeń komputerowych.

[37] Wniosek w sprawie rozporządzenia dotyczącego rozporządzenia ustanawiającego program kosmiczny Unii i Agencję Unii Europejskiej ds. Programu Kosmicznego, COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Utrzymuje się zagrożenie rozproszonymi atakami typu „odmowa usługi" (DDoS): główni dostawcy usług musieli stawić czoło masowym atakom typu DDoS takim jak atak na Amazon Web Services z lutego 2020 r.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

użytkownika, „na obrzeżach” sieci[41], ochrona centralnych punktów przestanie odgrywać główną rolę w cyberbezpieczeństwie[42].

W 2017 r. UE zaproponowała podejście do cyberbezpieczeństwa, którego centralnymi elementami były wzmocnienie odporności, szybkie reagowanie i skuteczne odstraszanie[43]. UE musi teraz zadbać, aby jej zdolności w zakresie cyberbezpieczeństwa nadążały za aktualnymi wyzwaniami, zarówno pod względem odporności, jak i reagowania. Konieczne jest, aby podejście to obejmowało naprawdę całe społeczeństwo, a instytucje, agencje i organy Unii, a także państwa członkowskie, przemysł, środowiska akademickie i osoby prywatne przywiązywały odpowiednią dużą wagę do cyberbezpieczeństwa[44]. W obszarach takich jak energetyka, usługi finansowe, transport czy zdrowie horyzontalne podejście należy z kolei uzupełnić sektorowymi strategiami dotyczącymi cyberbezpieczeństwa. Kolejny etap prac UE należy zaplanować wspólnie w ramach zmienionej europejskiej strategii w zakresie bezpieczeństwa cybernetycznego.

W ramach działań na rzecz poprawy cyberbezpieczeństwa, a także walki z terroryzmem, ekstremizmem, radykalizmem i zagrożeniami hybrydowymi należy szukać nowych, lepszych form współpracy między służbami wywiadowczymi, Centrum Analiz Wywiadowczych UE i innymi organizacjami zajmującymi się bezpieczeństwem.

W kontekście **infrastruktury 5G** uruchamianej obecnie w całej UE istnieje niebezpieczeństwo, że ewentualne systemowe zakłócenia o dużej skali będą miały szczególnie dotkliwe skutki, ponieważ wiele usług o krytycznym znaczeniu będzie potencjalnie uzależnionych od sieci 5G. W odpowiedzi na zalecenie Komisji z 2019 r.[45] państwa członkowskie podjęły konkretne działania w odniesieniu do kluczowych środków określonych w zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G[46].

Jedną z najważniejszych potrzeb w długim okresie jest stworzenie kultury **bezpieczeństwa cybernetycznego na etapie projektowania**. Bezpieczeństwo produktów i usług byłoby wówczas uwzględniane już na samym początku procesu ich tworzenia. Ważnym wkładem w osiągnięcie tego celu będzie wprowadzenie nowych ram certyfikacji cyberbezpieczeństwa na mocy aktu o cyberbezpieczeństwie[47]. Prace nad tymi ramami są już w toku: przygotowano dwa systemy certyfikacji, a priorytety dotyczące dalszych systemów zostaną określone jeszcze w tym roku. Kluczowe znaczenie w tym obszarze ma współpraca między

---

41 Przetwarzanie danych na obrzeżach sieci opiera się na rozproszonej, otwartej architekturze informatycznej, którą cechuje decentralizacja mocy obliczeniowej. Umożliwia ona działanie przenośnych urządzeń informatycznych i technologii, na których bazuje internet rzeczy. Dane nie są przekazywane do centrum danych, tylko przetwarzane na obrzeżach sieci – albo przez samo urządzenie, albo przez lokalny komputer lub serwer.

42 Komunikat w sprawie europejskiej strategii w zakresie danych, COM(2020) 66 final.

43 Wspólny komunikat pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej”, JOIN(2017) 450.

44 Raport Wspólnego Centrum Badawczego „Cybersecurity – our digital Anchor” [„Cyberbezpieczeństwo – nasza kotwica w cyberprzestrzeni”] przedstawia wiele aspektów ewolucji cyberbezpieczeństwa na przestrzeni ostatnich 40 lat.

45 Zalecenie Komisji w sprawie cyberbezpieczeństwa sieci 5G, C(2019) 2335. Zalecenie przewiduje przegląd w ostatnim kwartale 2020 r.

46 Zob. raport grupy współpracy ds. bezpieczeństwa sieci i informacji dotyczący wdrażania zestawu narzędzi na potrzeby cyberbezpieczeństwa, 24 lipca 2020 r.

47 Rozporządzenie 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie).

Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), organami ochrony danych i Europejską Radą Ochrony Danych[48].

Komisja uznała już za konieczne ustanowienie **wspólnej jednostki ds. cyberprzestrzeni** w celu organizowania i koordynacji współpracy operacyjnej. Współpraca ta mogłaby obejmować działający na szczeblu UE mechanizm wzajemnej pomocy w czasach kryzysu. Wykorzystując doświadczenia związane z wdrażaniem zalecenia w sprawie planu działania[49], wspólna jednostka ds. cyberprzestrzeni mogłaby budować zaufanie między poszczególnymi podmiotami tworzącymi europejski ekosystem cyberbezpieczeństwa i oferowałaby w ten sposób kluczową usługę państwom członkowskim. Komisja rozpocznie rozmowy z odpowiednimi interesariuszami (w pierwszej kolejności z państwami członkowskimi) i jeszcze przed końcem 2020 r. wytyczy jasny plan działania, cele pośrednie i ramy czasowe.

Duże znaczenie mają również wspólne dla wszystkich instytucji, organów i agencji Unii przepisy dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa. Celem powinno być stworzenie bezwzględnie obowiązujących, wysokich wspólnych standardów w zakresie bezpiecznej wymiany informacji oraz bezpieczeństwa infrastruktur i systemów cyfrowych we wszystkich instytucjach, organach i agencjach Unii. Te nowe ramy powinny stanowić podstawę silnej i sprawnej współpracy operacyjnej w dziedzinie cyberbezpieczeństwa pomiędzy instytucjami, organami i agencjami Unii. Kluczową rolę w tej współpracy odgrywałby zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE).

Ze względu na globalny charakter tego zagrożenia, stworzenie i utrzymanie silnych **partnerstw międzynarodowych** ma podstawowe znaczenie dla dalszego zapobiegania cyberatakom, powstrzymywania ich oraz reagowania na nie. Ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni („zestaw narzędzi dla dyplomacji cyfrowej”)[50] określają środki wspólnej polityki zagranicznej i bezpieczeństwa, w tym środki ograniczające (sankcje), za pomocą których można zwalczać działania szkodzące interesom politycznym i gospodarczym UE oraz naruszające jej bezpieczeństwo. UE powinna również zintensyfikować swoje działania prowadzone za pośrednictwem funduszy na rzecz rozwoju i współpracy, aby zapewnić budowanie zdolności państw partnerskich i pomagać im w ten sposób we wzmacnianiu ekosystemów cyfrowych, przyjmowaniu krajowych reform prawnych i przestrzeganiu standardów międzynarodowych. Wysiłki te zwiększają odporność całej społeczności oraz jej zdolność do przeciwdziałania zagrożeniom dla cyberbezpieczeństwa i skutecznego reagowania na nie. Działania te obejmują też w szczególności promowanie standardów UE i stosownych przepisów w celu zwiększenia cyberbezpieczeństwa sąsiedzkich krajów partnerskich[51].

Ochrona przestrzeni publicznej

Niedawne ataki terrorystyczne były wymierzone w **przestrzeń publiczną**, w tym w miejsca kultu i węzły transportowe, z uwagi na jej otwarty i ogólnodostępny charakter. Nasilenie

[48] Komunikat pt. „Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych”, COM(2020) 264.

[49] Zalecenie Komisji 2017/1584 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pl/pdf

[51] Zob. wytyczne dotyczące budowania przez UE zewnętrznych zdolności cyfrowych przyjęte w konkluzjach Rady z dnia 26 czerwca 2018 r.

terroryzmu motywowanego ekstremizmem na tle politycznym lub ideologicznym sprawiło, że zagrożenie atakami nabrało jeszcze bardziej poważnego charakteru. Sytuacja ta wymaga zarówno ściślejszej ochrony fizycznej przestrzeni publicznej, jak i odpowiednich systemów wykrywania, bez uszczerbku dla swobód obywatelskich[52]. Komisja zacieśni publiczno-prywatną współpracę w celu ochrony przestrzeni publicznej poprzez dostarczenie finansowania, wymianę doświadczeń i dobrych praktyk oraz konkretne wytyczne[53] i zalecenia[54]. Podejście to będzie również obejmować podnoszenie świadomości, wprowadzenie wymogów dotyczących działania sprzętu do wykrywania zagrożeń i testowanie tego sprzętu, a także dokładniejsze sprawdzanie przeszłości osób w celu zapobiegania zagrożeniom wewnętrznym. Ważnym aspektem, który wymaga refleksji, jest fakt, że członkowie mniejszości i grup podatnych na zagrożenia mogą szczególnie ucierpieć jako ofiary, np. ze względu na swoje wyznanie lub płeć, i wymagają w związku z tym szczególnej uwagi. Samorządy lokalne i regionalne mają do odegrania ważną rolę w poprawie bezpieczeństwa przestrzeni publicznej. Komisja przyczynia się również do wspierania innowacji miast w zakresie bezpieczeństwa przestrzeni publicznej[55]. Uruchomienie w listopadzie 2018 r. partnerstwa na rzecz bezpieczeństwa przestrzeni publicznej w ramach Nowej agendy miejskiej[56] świadczy o tym, że państwa członkowskie, Komisja i miasta starają się radzić sobie lepiej z zagrożeniami dla bezpieczeństwa w przestrzeni miejskiej.

Rynek **dronów**, które mają wiele pożytecznych i zgodnych z prawem zastosowań, stale się rozwija. Urządzenia te mogą być jednak używane przez przestępców i terrorystów do celów niezgodnych z prawem. Szczególnie narażone na atak za pomocą dronów są przestrzenie publiczne. Ataki mogą być wymierzone w pojedyncze osoby, zgromadzenia, infrastrukturę krytyczną, organy ścigania, granice państw lub przestrzenie publiczne. Wiedza na temat sposobów wykorzystywania dronów w konfliktach zbrojnych trafia do Europy albo bezpośrednio, wraz z powracającymi zagranicznymi bojownikami terrorystycznymi, albo przez internet. Przepisy opracowane już przez Europejską Agencję Bezpieczeństwa Lotniczego stanowią ważny pierwszy krok. Dotyczą one m.in. obszarów takich jak rejestracja operatorów dronów i obowiązkowa zdalna identyfikacja dronów. Konieczne są jednak dalsze działania, ponieważ drony stają się coraz powszechniej dostępne, przystępne cenowo i funkcjonalne. Dodatkowe działania mogłyby obejmować wymianę informacji, opracowanie wytycznych i dobrych praktyk do powszechnego użytku, w tym przez organy ścigania, czy też testowanie na szerszą skalę środków ochrony przed dronami[57]. Należy

[52] W tym kontekście należy przyjrzeć się szczególnie systemom identyfikacji biometrycznej na odległość. Pierwotne stanowisko Komisji przedstawiono w jej białej księdze z dnia 19 lutego 2020 r. w sprawie sztucznej inteligencji, COM(2020) 65.

[53] Na przykład wytyczne dotyczące wyboru odpowiednich barier bezpieczeństwa w celu ochrony przestrzeni publicznej (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Wytyczne dotyczące dobrych praktyk znajdują się w dokumencie SWD(2019) 140. Jedna z sekcji tego dokumentu jest poświęcona współpracy publiczno-prywatnej. Szczególny nacisk na zacieśnianie współpracy publiczno-prywatnej kładziony jest w ramach finansowania z Funduszu Bezpieczeństwa Wewnętrznego – części dotyczącej współpracy policyjnej.

[55] Trzy miasta (Pireus w Grecji, Tampere w Finlandii i Turyn we Włoszech) będą testować nowe rozwiązania w ramach innowacyjnych działań miejskich przy współfinansowaniu z Europejskiego Funduszu Rozwoju Regionalnego (EFRR).

[56] Agenda miejska dla UE stanowi nową, wielopoziomową metodę pracy i sprzyja współdziałaniu państw członkowskich, miast, Komisji Europejskiej i innych interesariuszy w celu pobudzenia wzrostu gospodarczego i innowacji oraz polepszenia komfortu życia w miastach Europy, a także w celu identyfikowania i pokonywania wyzwań społecznych.

[57] Niedawno ustanowiono wieloletni program testów w tym obszarze, który ma pomóc państwom członkowskim opracować wspólną metodykę i platformę testową.

również przeanalizować bardziej szczegółowo kwestie prywatności i ochrony danych w kontekście używania dronów w przestrzeni publicznej.

Główne działania
• Przepisy dotyczące ochrony i odporności infrastruktury krytycznej • Przegląd dyrektywy w sprawie bezpieczeństwa sieci i systemów informacyjnych • Inicjatywa na rzecz zwiększenia odporności operacyjnej sektora finansowego • Ochrona i cyberbezpieczeństwo krytycznej infrastruktury energetycznej oraz kodeks sieci dotyczący cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej • Europejska strategia w zakresie bezpieczeństwa cybernetycznego • Dalsze kroki w celu stworzenia wspólnej jednostki ds. cyberprzestrzeni • Wspólne dla wszystkich instytucji, organów i agencji Unii przepisy dotyczące bezpieczeństwa informacji i cyberbezpieczeństwa • Wzmożona współpraca w celu ochrony przestrzeni publicznej, w tym miejsc kultu • Dzielenie się najlepszymi praktykami dotyczącymi przeciwdziałania wykorzystywaniu dronów do celów niezgodnych z prawem

2. Działanie w obliczu zmieniających się zagrożeń

Cyberprzestępczość

Technika otwiera nowe możliwości przed społeczeństwami oraz oferuje nowatorskie narzędzia wymiarowi sprawiedliwości i organom ścigania. Jednocześnie otwiera ona też drzwi przestępcom. Rośnie plaga złośliwego oprogramowania, a hakerzy dopuszczają się coraz częściej kradzieży danych osób prywatnych lub przedsiębiorstw i blokowania działalności cyfrowej usługodawców, co prowadzi do szkód finansowych lub nadszarpnięcia reputacji. Pierwszą linią obrony jest odporne środowisko, które powstaje dzięki solidnemu cyberbezpieczeństwu. Organy ścigania potrzebują do swojej pracy jasnych przepisów regulujących prowadzenie dochodzeń w sprawach o przestępstwa komputerowe i ściganie takich przestępstw oraz zapewniających niezbędną ochronę ofiarom. Aby zapewnić im takie przepisy, należy oprzeć się na pracach Wspólnej Grupy Zadaniowej ds. Przeciwdziałania Cyberprzestępczości działającej w ramach Europolu i na protokole działań w zakresie egzekwowania prawa w sytuacjach kryzysowych, który powstał w celu koordynowania reakcji na ataki cybernetyczne na dużą skalę. Kluczowe znaczenie mają również skuteczne mechanizmy umożliwiające tworzenie partnerstw publiczno-prywatnych i współpracę między tymi dwoma sektorami.

Jednocześnie walka z cyberprzestępczością powinna stać się priorytetem komunikacji strategicznej w całej UE: należy ostrzegać Europejczyków o zagrożeniach i informować ich, w jaki sposób mogą się przed nimi chronić. Działanie to powinno stanowić element proaktywnego podejścia. Konieczne jest również pełne wdrożenie już istniejących ram prawnych[58]: w stosownych przypadkach Komisja będzie gotowa wszcząć postępowanie w sprawie uchybienia zobowiązaniom państwa członkowskiego i będzie również dokonywać regularnego przeglądu tych ram, aby zapewnić ich adekwatność. Komisja zbada również, wspólnie z Europolem i Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, możliwość wprowadzenia unijnego systemu wczesnego ostrzegania, który zapewniałby przepływ informacji i szybkie reagowanie na cyberprzestępstwa.

[58] Dyrektywa 2013/40/UE dotycząca ataków na systemy informatyczne.

Cyberprzestępczość stanowi globalny problem, dlatego walka z nią wymaga skutecznej współpracy międzynarodowej. UE popiera Konwencję o cyberprzestępczości uchwaloną przez Radę Europy w Budapeszcie, która stanowi skuteczne i ugruntowane ramy prawne. Pomagają one wszystkim państwom określić, jakie systemy i kanały komunikacji są im potrzebne do skutecznej współpracy.

Niemal połowa obywateli UE obawia się, że ich dane zostaną wykorzystane niezgodnie z przeznaczeniem[59]; poważny niepokój budzi również **kradzież tożsamości**[60]. Przestępstwo to może wiązać się z uzurpowaniem tożsamości w celu uzyskania korzyści finansowej, ale może też prowadzić do poważnych szkód w życiu osobistym i cierpień psychicznych ofiary – w niektórych przypadkach treści umieszczone w internecie przez złodzieja tożsamości pozostają dostępne przez wiele lat. Komisja zbada praktyczne możliwości ochrony ofiar przed wszelkimi formami kradzieży tożsamości, uwzględniając przy tym zapowiedzianą inicjatywę na rzecz europejskiej tożsamości cyfrowej[61].

Aby zwalczać cyberprzestępczość, trzeba myśleć perspektywicznie. Podczas gdy ogół ludzi wykorzystuje nowe rozwiązania technologiczne do wzmacniania gospodarki i społeczeństwa, w rękach przestępców służą one do wyrządzania szkód. Mogą oni na przykład wykorzystywać sztuczną inteligencję do wykrywania i odczytywania haseł, tworzenia złośliwego oprogramowania oraz manipulacji obrazem i dźwiękiem w celu dokonania kradzieży tożsamości lub popełnienia oszustwa.

Nowoczesne egzekwowanie prawa

Pracownicy organów ścigania i osoby wykonujące zawody prawnicze muszą dostosować się do nowej technologii. W świetle rozwoju technicznego i pojawiających się zagrożeń jest konieczne, aby organy ścigania miały dostęp do nowych narzędzi, nabywały nowe umiejętności i rozwijały alternatywne techniki dochodzeniowe. W celu uzupełnienia działań ustawodawczych mających na celu poprawę transgranicznego dostępu do elektronicznego materiału dowodowego w postępowaniach przygotowawczych, UE może pomóc organom ścigania rozwinąć zdolności niezbędne do identyfikowania, zabezpieczania i odczytywania danych potrzebnych do prowadzenia dochodzeń w sprawie przestępstw oraz do wykorzystywania tych danych jako dowodów w sądzie. Komisja zbada, w jaki sposób można **zwiększyć zdolności organów ścigania w zakresie dochodzeń w sprawach o przestępstwa komputerowe** i optymalnie wykorzystywać prace badawczo-rozwojowe do tworzenia nowych narzędzi dla organów ścigania oraz jakie szkolenia mogą zapewnić odpowiednie umiejętności pracownikom organów ścigania i wymiaru sprawiedliwości. Działania Komisji będą też obejmować rygorystyczne oceny naukowe i opracowanie metod testowania za pośrednictwem jej Wspólnego Centrum Badawczego.

Wspólne podejścia mogą przyczynić się ponadto do tego, że **sztuczna inteligencja, zdolności do działania w przestrzeni kosmicznej, duże zbiory danych** i **obliczenia wielkiej skali zostaną włączone** w politykę bezpieczeństwa w sposób zapewniający z jednej strony skuteczną walkę z przestępczością, a z drugiej strony poszanowanie praw

[59] 46 % (badanie Eurobarometr ze stycznia 2020 r. dotyczące stosunku Europejczyków do cyberbezpieczeństwa).

[60] Ogromna większość (95 %) respondentów w badaniu Eurobarometr z 2018 r. pt. „Postawy Europejczyków wobec bezpieczeństwa w internecie" postrzegała kradzież tożsamości jako poważne przestępstwo, a siedmiu na dziesięciu respondentów – jako bardzo poważne przestępstwo. Opublikowane w styczniu 2020 r. badanie Eurobarometr potwierdziło zaniepokojenie cyberprzestępczością, oszustwami internetowymi i kradzieżami tożsamości: dwie trzecie respondentów obawiało się oszustw bankowych (67 %) albo kradzieży tożsamości (66 %).

[61] Komunikat z dnia 19 lutego 2020 r. w sprawie kształtowania cyfrowej przyszłości Europy, COM(2020) 67.

podstawowych. Sztuczna inteligencja może stanowić potężne narzędzie do zwalczania przestępczości, oferując ogromne zdolności dochodzeniowe dzięki analizie dużych ilości informacji oraz wykrywaniu w nich prawidłowości i anomalii[62]. Może ona również służyć do konkretnych zadań, takich jak pomoc w identyfikacji treści o charakterze terrorystycznym w internecie i wykrywaniu podejrzanych transakcji sprzedaży produktów niebezpiecznych czy oferowanie pomocy obywatelom w sytuacjach kryzysowych. Aby wykorzystać ten potencjał, badacze, innowatorzy i użytkownicy sztucznej inteligencji powinni otrzymać dostęp do odpowiednich mechanizmów zarządzania i infrastruktury technicznej, przy aktywnym udziale sektora prywatnego i środowiska akademickiego. Konieczne jest również zachowanie najwyższych standardów przestrzegania praw podstawowych i jednoczesne zapewnienie skutecznej ochrony obywateli. Należy dopilnować w szczególności, aby zautomatyzowane decyzje mające wpływ na osoby fizyczne były kontrolowane przez ludzi i były zgodne z odpowiednimi przepisami prawa UE, które mają zastosowanie[63].

W około 85 % dochodzeń w sprawie poważnych przestępstw potrzebne są informacje i dowody elektroniczne, a 65 % wszystkich wniosków o ich udostępnienie trafia do dostawców usług mających siedzibę w innym kraju[64]. Ponieważ śladów materialnych przestępstw szuka się coraz częściej w internecie, a nie w świecie materialnym, rośnie dystans między organami ścigania a przestępcami, jeśli chodzi o zdolność działania w środowisku cyfrowym. Konieczne jest wprowadzenie jasnych przepisów dotyczących transgranicznego dostępu do elektronicznego materiału dowodowego w postępowaniach przygotowawczych. Dlatego tak ważne jest szybkie przyjęcie przez Parlament Europejski i Radę wniosków w sprawie elektronicznych materiałów dowodowych, które udostępnią to skuteczne narzędzie osobom wykonującym zawody prawnicze. Kluczowe jest także zapewnienie transgranicznego dostępu do elektronicznych materiałów dowodowych w drodze wielostronnych i dwustronnych negocjacji międzynarodowych. Umożliwi to ustanowienie spójnych przepisów na szczeblu międzynarodowym[65].

Dostęp do dowodów cyfrowych zależy również od dostępności informacji. Jeżeli dane są usuwane zbyt szybko, mogą zniknąć ważne dowody, a wraz z nimi możliwość zidentyfikowania i zlokalizowania osób podejrzanych i sieci przestępczych (a także ofiar). W przypadku zatrzymywania danych pojawiają się natomiast wątpliwości dotyczące ochrony prywatności. Komisja określi dalsze działania dotyczące zatrzymywania danych w oparciu o wyroki, jakie zapadną w sprawach toczących się przed Trybunałem Sprawiedliwości UE.

Dostęp do informacji na temat rejestracji nazw domen internetowych („danych WHOIS”)[66] jest ważny do celów postępowań przygotowawczych, cyberbezpieczeństwa i ochrony konsumentów. Dostęp do tych informacji staje się jednak trudniejszy, ponieważ Internetowa

---

[62] Na przykład w przypadku przestępstw finansowych.

[63] Rozumie się przez to zgodność z obowiązującym prawodawstwem, w tym z rozporządzeniem (UE) 2016/679 (ogólnym rozporządzeniem o ochronie danych) i z dyrektywą (UE) 2016/680 (dyrektywą o ochronie danych w sprawach karnych), która reguluje przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar.

[64] Dokument roboczy służb Komisji SWD(2018) 118 final.

[65] W szczególności drugi protokół dodatkowy do budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości i porozumienie między UE a Stanami Zjednoczonymi w sprawie transgranicznego dostępu do elektronicznych materiałów dowodowych.

[66] Dane te są przechowywane w bazach danych prowadzonych przez 2 500 operatorów rejestru i rejestratorów na całym świecie.

Korporacja ds. Nadanych Nazw i Numerów (ICANN) nie przyjęła jeszcze nowej polityki dotyczącej WHOIS. Komisja będzie dalej współpracować z ICANN i ze społecznością obejmującą wielu interesariuszy w celu zapewnienia, by wnioskodawcy – w tym organy ścigania – ubiegający się o prawnie uzasadniony dostęp do danych WHOIS mogli go sprawnie uzyskać zgodnie z unijnymi i międzynarodowymi przepisami o ochronie danych. Współpraca ta będzie obejmować ocenę możliwych rozwiązań, w tym ustalenie, czy konieczne jest doprecyzowanie przepisów w sprawie dostępu do takich informacji.

Organy ścigania i organy wymiaru sprawiedliwości muszą być w stanie uzyskać dostęp do niezbędnych danych i dowodów również po pełnym wdrożeniu w UE **architektury sieci 5G na potrzeby telefonii komórkowej**, w sposób zapewniający poszanowanie poufności komunikacji. Komisja będzie wspierać wzmocnione i skoordynowane podejście podczas tworzenia międzynarodowych norm oraz określania najlepszych praktyk, procedur i technicznej interoperacyjności w kluczowych obszarach technologii, takich jak sztuczna inteligencja, internet rzeczy czy *blockchain*.

Prowadząc dochodzenia w sprawie różnych form przestępczości i terroryzmu, śledczy mają dziś często do czynienia z **zaszyfrowanymi informacjami**. Szyfrowanie ma podstawowe znaczenie dla świata cyfrowego, ponieważ zabezpiecza systemy cyfrowe i transakcje oraz chroni szereg praw podstawowych, w tym wolność wypowiedzi, prywatność i ochronę danych. W rękach przestępców szyfrowanie może jednak służyć do ukrywania ich tożsamości i treści komunikacji. Komisja zbada, jakie zrównoważone rozwiązania techniczne, operacyjne i prawne odpowiadają na te wyzwania, i wesprze je. Będzie też promować podejście, które zapewnia jednocześnie skuteczność szyfrowania transmisji w celu ochrony prywatności i bezpieczeństwa łączności oraz skuteczną walkę z przestępczością i terroryzmem.

Zwalczanie nielegalnych treści w internecie

Aby środowisko online było podobnie bezpieczne jak otoczenie fizyczne, konieczne jest kontynuowanie działań **zwalczających nielegalne treści w internecie**. Wiele poważnych zagrożeń dla obywateli, takich jak terroryzm, ekstremizm czy niegodziwe traktowanie dzieci w celach seksualnych, szerzy się głównie w środowisku cyfrowym: walka z nimi wymaga konkretnych działań i ram zapewniających poszanowanie praw podstawowych. Niezbędnym pierwszym krokiem jest szybkie zakończenie negocjacji w sprawie proponowanych przepisów dotyczących internetowych treści o charakterze terrorystycznym[67] oraz zapewnienie ich wdrożenia. Pomocne w walce z wykorzystywaniem internetu przez terrorystów, brutalnych ekstremistów i przestępców do celów niezgodnych z prawem byłoby zacieśnienie dobrowolnej współpracy między organami ścigania a sektorem prywatnym w ramach **Forum UE ds. Internetu**. Działająca w Europolu unijna jednostka ds. zgłaszania podejrzanych treści w internecie będzie nadal odgrywać kluczową rolę w monitorowaniu aktywności grup terrorystycznych w internecie i reakcji platform internetowych na tę aktywność[68], a także w dalszym rozwijaniu **unijnego protokołu kryzysowego**[69]. Oprócz tego Komisja będzie dalej współpracować z partnerami międzynarodowymi, w tym poprzez uczestnictwo w **Globalnym Internetowym Forum Przeciwdziałania Terroryzmowi**, w celu rozwiązania tych problemów na szczeblu światowym. Kontynuowane będą prace

[67] Wniosek z dnia 12 września 2018 r. dotyczący zapobiegania rozpowszechnianiu w internecie treści o charakterze terrorystycznym, COM(2018) 640.

[68] Europol, listopad 2019 r.

[69] A Europe that protects - EU Crisis Protocol: responding to terrorist content online [Europa, która chroni – unijny protokół kryzysowy: reagowanie na treści o charakterze terrorystycznym publikowane online]. (październik 2019 r.).

wspierające opracowywanie alternatywnych i przeciwstawnych narracji w ramach programu na rzecz wzmacniania społeczeństwa obywatelskiego[70].

Aby zapobiegać rozprzestrzenianiu się mowy nienawiści w internecie i przeciwdziałać temu problemowi, Komisja wprowadziła w 2016 r. Kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie, zawierający dobrowolne zobowiązanie platform internetowych do usuwania takich treści. Niedawna ocena pokazuje, że przedsiębiorstwa sprawdzają 90 % zgłoszonych treści w ciągu 24 godzin i usuwają 71 % treści uznanych za nielegalne nawoływanie do nienawiści. Platformy muszą jednak dalej dążyć do zwiększenia przejrzystości i poprawy informacji zwrotnych dla użytkowników oraz zapewnić spójną ocenę zgłoszonych treści[71].

Forum UE ds. Internetu ułatwi również wymianę informacji na temat już istniejących i rozwijanych technologii pomocnych w walce z niegodziwym traktowaniem dzieci w internecie w celach seksualnych. Zapobieganie temu przestępstwu stanowi centralny element nowej strategii mającej na celu skuteczniejsze **zwalczanie niegodziwego traktowania dzieci w celach seksualnych**[72] dzięki maksymalnemu wykorzystaniu narzędzi dostępnych na szczeblu UE. Przedsiębiorstwa muszą być w stanie kontynuować prace nad wykrywaniem i usuwaniem materiałów internetowych prezentujących seksualne wykorzystywanie dziecka, a w świetle szkód powodowanych przez takie materiały niezbędne są ramy prawne jasne określające stały obowiązek zwalczania tego problemu. W strategii zapowiedziane zostaną również prace Komisji nad przepisami sektorowymi mającymi na celu skuteczniejsze zwalczanie niegodziwego traktowania dzieci w internecie w celach seksualnych, przy pełnym poszanowaniu praw podstawowych.

Jeżeli chodzi o szersze kwestie dotyczące internetu, akt prawny o usługach cyfrowych, który zostanie wkrótce przedstawiony, doprecyzuje i zmodernizuje przepisy dotyczące odpowiedzialności i bezpieczeństwa w zakresie usług cyfrowych oraz usunie przepisy zniechęcające do podejmowania działań w celu wyeliminowania nielegalnych treści, towarów lub usług.

Oprócz tego Komisja będzie kontynuować rozmowy z partnerami międzynarodowymi i **Globalnym Internetowym Forum Przeciwdziałania Terroryzmowi**, m.in. za pośrednictwem niezależnego komitetu doradczego, w celu rozwiązania tych problemów na szczeblu światowym z poszanowaniem europejskich wartości i praw podstawowych. Należy również uwzględnić nowe zjawiska, takie jak algorytmy czy gry online[73].

Zagrożenia hybrydowe

Skala i różnorodność zagrożeń hybrydowych w dzisiejszym świecie jest bezprecedensowa. Kryzys związany z COVID-19 jeszcze jaskrawiej je uwydatnił – pewne państwa i podmioty niepaństwowe próbowały instrumentalnie wykorzystywać pandemię, głównie manipulując środowiskiem informacyjnym i próbując naruszać infrastrukturę podstawową. Grozi to osłabieniem spójności społecznej i podważeniem zaufania do instytucji UE i rządów państw członkowskich.

---

[70] Powiązane z pracami w ramach programu upowszechniania wiedzy o radykalizacji postaw, zob. sekcja IV pkt 3 poniżej.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Strategia UE na rzecz skuteczniejszej walki z niegodziwym traktowaniem dzieci w celach seksualnych, COM(2020) 607.

[73] Terroryści coraz częściej wykorzystują systemy platform do gier do przesyłania sobie wiadomości, a młodzi terroryści grają w gry wideo rekonstruujące brutalne ataki.

Podejście UE do zagrożeń hybrydowych określono we wspólnych ramach z 2016 r.[74] i we wspólnym komunikacie z 2018 r. w sprawie zwiększenia odporności na zagrożenia hybrydowe[75]. W działaniach na szczeblu UE wykorzystuje się obszerny zestaw narzędzi uwzględniający powiązanie między wymiarem wewnętrznym i zewnętrznym, opierający się na podejściu obejmującym całe społeczeństwo oraz na ścisłej współpracy z partnerami strategicznymi, w szczególności NATO i G7. Wraz z niniejszą strategią publikowane jest sprawozdanie z wdrażania unijnego podejścia do zagrożeń hybrydowych[76]. Na podstawie wykazu[77] przedstawianego wraz z niniejszą strategią służby Komisji i Europejska Służba Działań Zewnętrznych utworzą **platformę internetową o ograniczonym dostępie**, dostarczającą państwom członkowskim informacji o narzędziach i środkach przeciwdziałania zagrożeniom hybrydowym na szczeblu UE.

Jakkolwiek odpowiedzialność za przeciwdziałanie zagrożeniom hybrydowym, ze względu na nieodłączne powiązania z krajową polityką bezpieczeństwa i obrony, spoczywa przede wszystkim na państwach członkowskich, to niektóre aspekty podatności na zagrożenia są wspólne dla wszystkich państw członkowskich, a zasięg pewnych zagrożeń – np. działań wymierzonych w transgraniczne sieci lub infrastrukturę – wykracza poza granice państwowe. Komisja i Wysoki Przedstawiciel określą podejście UE do zagrożeń hybrydowych, które będzie płynnie łączyć wymiar zewnętrzny i wewnętrzny oraz zagadnienia krajowe i ogólnounijne. Musi ono obejmować pełne spektrum działań – od wczesnego wykrywania, analizy i kształtowania świadomości, poprzez budowanie odporności i zapobieganie, po reagowanie na sytuacje kryzysowe i zarządzanie skutkami.

Oprócz skuteczniejszej realizacji działań – z uwagi na to, że zagrożenia hybrydowe nieustannie się zmieniają, szczególny nacisk zostanie położony na **uwzględnienie zagrożeń hybrydowych w głównym nurcie kształtowania polityki**, aby dotrzymać kroku ich dynamicznemu rozwojowi i aby żadna potencjalnie istotna inicjatywa nie została przeoczona. Skutki nowych inicjatyw będą także oceniane przez pryzmat zagrożeń hybrydowych. Dotyczy to również inicjatyw w dziedzinach, które do tej pory nie były uwzględniane w kontekście zwalczania zagrożeń hybrydowych, jak edukacja, technologia i badania naukowe. W ramach takiego podejścia wskazane byłoby czerpanie z efektów prac w zakresie konceptualizacji zagrożeń hybrydowych, co dałoby kompleksowy obraz rozmaitych narzędzi wykorzystywanych przez przeciwników[78]. Celem powinno być zapewnienie, aby proces decyzyjny opierał się na regularnie uzyskiwanych, kompleksowych informacjach wywiadowczych na temat rozwoju zagrożeń hybrydowych. Będzie to wymagać wykorzystywania na dużą skalę danych wywiadowczych państw członkowskich oraz dalszego zacieśniania współpracy z właściwymi służbami państw członkowskich za pośrednictwem Centrum Analiz Wywiadowczych UE (INTCEN).

W celu zwiększania **orientacji sytuacyjnej** służby Komisji i Europejska Służba Działań Zewnętrznych zbadają możliwości usprawnienia przepływu informacji z różnych źródeł,

---

[74] Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, JOIN(2016) 18.

[75] Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe, JOIN(2018) 16.

[76] SWD(2020) 153 – Sprawozdanie w sprawie wdrażania wspólnych ram dotyczących przeciwdziałania zagrożeniom hybrydowym z 2016 r. oraz wspólnego komunikatu z 2018 r. w sprawie zwiększenia odporności i wzmocnienia zdolności reagowania na zagrożenia hybrydowe.

[77] SWD(2020) 152 – Wykaz działań służących zwiększeniu odporności na zagrożenia hybrydowe i przeciwdziałaniu im.

[78] „The Landscape of Hybrid Threats: A conceptual Model" [„Krajobraz zagrożeń hybrydowych: model pojęciowy"], JRC117280, opracowanie Wspólnego Centrum Badawczego i Centrum Doskonałości ds. Zwalczania Zagrożeń Hybrydowych.

w tym państw członkowskich, a także agencji UE, takich jak ENISA, Europol i Frontex. Centralnym punktem UE do spraw oceny zagrożeń hybrydowych pozostanie Komórka UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych. Zasadnicze znaczenie dla zapobiegania zagrożeniom hybrydowym i ochrony przed nimi ma **budowanie odporności**. Niezbędne jest zatem systematyczne śledzenie i obiektywny pomiar postępów w tym zakresie. Pierwszym krokiem będzie określenie wyjściowych poziomów odporności sektorowej państw członkowskich oraz instytucji i organów UE na zagrożenia hybrydowe. Wreszcie, w celu zwiększenia **gotowości do reagowania na kryzysy hybrydowe**, należy dokonać przeglądu obecnego protokołu, jak przewidziano to w unijnym podręczniku taktycznym z 2016 r.[79], biorąc pod uwagę szerszą perspektywę oraz rozpatrywane obecnie wzmocnienie unijnego systemu reagowania kryzysowego[80]. Celem jest maksymalizacja skuteczności działań UE poprzez szybkie łączenie reakcji sektorowych oraz zapewnianie płynnej współpracy z naszymi partnerami, przede wszystkim z NATO.

Główne działania
• Zadbanie o to, aby przepisy dotyczące cyberprzestępczości były wdrażane i adekwatne do zakładanych celów • Strategia skuteczniejszego zwalczania niegodziwego traktowania dzieci w celach seksualnych • Wnioski w sprawie wykrywania i usuwania materiałów prezentujących seksualne wykorzystywanie dziecka • Ogólnounijne podejście do przeciwdziałania zagrożeniom hybrydowym • Przegląd unijnego protokołu operacyjnego do celów przeciwdziałania zagrożeniom hybrydowym (unijnego podręcznika taktycznego) • Ocena sposobów zwiększenia zdolności organów ścigania w dochodzeniach w sprawach o przestępstwa komputerowe

3. Ochrona Europejczyków przed terroryzmem i przestępczością zorganizowaną

Terroryzm i radykalizacja postaw

Zagrożenie terrorystyczne w UE jest nadal wysokie. Choć ogólnie zamachów jest mniej, to nadal mogą one mieć katastrofalne skutki. Ponadto radykalizacja postaw może prowadzić, w szerszym ujęciu, do polaryzacji i destabilizacji spójności społecznej. Główna odpowiedzialność za zwalczanie terroryzmu i radykalizacji nadal spoczywa na państwach członkowskich. Niemniej jednak w obliczu wciąż rosnącego transgranicznego i międzysektorowego wymiaru zagrożenia konieczne jest rozwijanie współpracy i koordynacji w UE. Skuteczne wdrażanie unijnych przepisów o zwalczaniu terroryzmu, w tym środków ograniczających[81], ma priorytetowe znaczenie. Jednym z celów pozostaje

[79] Unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym (unijny podręcznik taktyczny), SWD(2016) 227.

[80] Po wideokonferencji w dniu 26 marca 2020 r. członkowie Rady Europejskiej przyjęli oświadczenie w sprawie działań UE w odpowiedzi na pandemię COVID-19, zwracając się do Komisji o przedstawienie wniosków zmierzających ku bardziej ambitnemu i szerzej zakrojonemu systemowi zarządzania kryzysowego w UE.

[81] W celu zwalczania terroryzmu Rada przyjęła środki ograniczające wobec ISIL (Daisz) i Al-Kaidy oraz szczególne środki ograniczające skierowane przeciwko określonym osobom i podmiotom. Przegląd wszystkich środków ograniczających ilustruje „mapa sankcji UE" (https://www.sanctionsmap.eu/#/main).

objęcie transgranicznych przestępstw terrorystycznych zakresem kompetencji Prokuratury Europejskiej.

Zwalczanie terroryzmu rozpoczyna się od eliminowania jego pierwotnych przyczyn. Polaryzacja społeczeństwa, realna lub postrzegana dyskryminacja oraz inne czynniki psychologiczne i socjologiczne mogą zwiększać podatność ludzi na radykalny dyskurs. W tym kontekście przeciwdziałanie **radykalizacji** idzie w parze ze wspieraniem spójności społecznej na szczeblu lokalnym, krajowym i europejskim. W ciągu ostatniej dekady opracowano szereg skutecznych inicjatyw i polityk, w szczególności za pośrednictwem sieci upowszechniania wiedzy o radykalizacji postaw oraz inicjatywy „Miasta UE przeciwko radykalizacji postaw"[82]. Czas teraz rozważyć działania na rzecz skuteczniejszego przeciwdziałania radykalizacji za pomocą polityk, inicjatyw i funduszy UE. Działania takie mogą wspierać rozwój zdolności i umiejętności, sprzyjać zacieśnianiu współpracy i powiększaniu wiedzy oraz pomagać w ocenie postępów, a uczestniczyć w nich powinni wszyscy interesariusze, w tym pracownicy pierwszego kontaktu, decydenci polityczni i środowisko akademickie[83]. W zapobieganiu radykalizacji postaw pomocne mogą być „miękkie" środki w takich dziedzinach polityki, jak edukacja, kultura, młodzież i sport, które stwarzają możliwości dla zagrożonej młodzieży i sprzyjają spójności wewnątrz UE[84]. Obszary priorytetowe to m.in. działania w zakresie wczesnego wykrywania ryzyka i zarządzania nim, budowanie odporności, wysiłki na rzecz zaprzestania stosowania przemocy przez środowiska ekstremistyczne, a także resocjalizacja i reintegracja społeczna.

Terroryści próbują nabywać materiały **chemiczne, biologiczne, radiologiczne i jądrowe** (CBRJ)[85] i przekształcać w broń, rozwijając wiedzę i możliwości potrzebne do tego celu[86]. W propagandzie terrorystycznej potencjał ataków przy użyciu materiałów CBRJ odgrywa eksponowaną rolę. Szkody mogą być ogromne, a więc konieczne jest poświęcenie tym zagadnieniom szczególnej uwagi. Opierając się na podejściu stosowanym przy regulowaniu dostępu do prekursorów materiałów wybuchowych, Komisja rozważy ograniczenie dostępności niektórych niebezpiecznych chemikaliów, które mogą być wykorzystywane do przeprowadzania ataków. Kluczowe znaczenie będzie mieć również rozwój zdolności reagowania UE w dziedzinie ochrony ludności (rescEU) w aspekcie CBRJ. Istotna jest także współpraca z państwami trzecimi, służąca rozwijaniu wspólnej kultury bezpieczeństwa i ochrony w zakresie CBRJ, przy pełnym wykorzystaniu unijnych globalnych centrów doskonałości ds. CBRJ. Współpraca ta będzie obejmować krajowe oceny braków i ryzyka, wsparcie dla krajowych i regionalnych planów działania w obszarze CBRJ, wymianę dobrych praktyk oraz działania na rzecz budowania zdolności w zakresie CBRJ.

UE opracowała najbardziej zaawansowane na świecie przepisy służące ograniczeniu dostępu do **prekursorów materiałów wybuchowych**[87] i wykrywaniu podejrzanych transakcji

[82] Inicjatywa pilotażowa „Miasta UE przeciwko radykalizacji postaw" ma dwojaki cel: wspieranie wymiany wiedzy i doświadczeń między miastami UE oraz gromadzenie informacji zwrotnych o najlepszych sposobach wspierania lokalnych społeczności na szczeblu UE.

[83] Działania mogą otrzymywać finansowanie m.in. w ramach Europejskiego Funduszu Bezpieczeństwa oraz programu „Obywatelstwo".

[84] M.in. działania UE w postaci wirtualnych wymian Erasmus+ lub e-twinningu.

[85] Przykładowo w ciągu ostatnich dwóch lat odnotowano kilka prób wykorzystania czynników biologicznych (zazwyczaj toksyn pochodzenia roślinnego) w Europie (we Francji, Niemczech i Włoszech) i poza nią (Tunezja, Indonezja).

[86] Rada przyjęła środki ograniczające rozprzestrzenianie i stosowanie broni chemicznej.

[87] Czyli chemikaliów, które można nielegalnie wykorzystać do wytworzenia materiałów wybuchowych domowym sposobem. Są one regulowane rozporządzeniem (UE) 2019/1148 w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych.

zmierzających do budowy improwizowanych urządzeń wybuchowych. Zagrożenie związane ze stosowaniem materiałów wybuchowych wytwarzanych domowym sposobem jest jednak nadal wysokie, a materiały takie są stosowane w wielu zamachach w całej UE[88]. Pierwszym krokiem musi być wdrażanie przepisów, a także zapewnienie, by środowisko internetowe nie umożliwiało omijania kontroli.

Ważnym elementem polityki zwalczania terroryzmu jest również skuteczne ściganie sprawców przestępstw terrorystycznych, w tym **zagranicznych bojowników terrorystycznych** działających obecnie w Syrii i Iraku. Co prawda tym zajmują się w głównej mierze państwa członkowskie, jednak w sprostaniu wspólnym wyzwaniom mogą im pomóc unijna koordynacja i wsparcie. Istotne w tym kontekście są trwające działania na rzecz pełnego wdrożenia przepisów o bezpieczeństwie granic[89] i jak największego wykorzystania wszystkich odnośnych baz danych UE w celu wymiany informacji na temat znanych osób podejrzanych. Oprócz identyfikacji osób stanowiących wysokie ryzyko konieczna jest polityka w zakresie reintegracji i resocjalizacji. Współpraca międzyzawodowa, m.in. z personelem więziennym i kuratorskim, przyczyni się do lepszego zrozumienia – z perspektywy wymiaru sprawiedliwości – procesów radykalizacji postaw prowadzących do brutalnego ekstremizmu oraz wypracowania w tym sektorze podejścia do wydawania wyroków skazujących i stosowania rozwiązań alternatywnych wobec pozbawiania wolności.

Wyzwania dotyczące zagranicznych bojowników terrorystycznych unaoczniają powiązania **bezpieczeństwa zewnętrznego** z wewnętrznym. Współpraca w zakresie zwalczania terroryzmu oraz zapobiegania radykalizacji postaw i brutalnemu ekstremizmowi i przeciwdziałania im ma kluczowe znaczenie dla bezpieczeństwa wewnątrz UE[90]. Konieczne są dalsze działania w celu rozwijania partnerstw antyterrorystycznych i współpracy z krajami w sąsiedztwie UE i poza nim, z wykorzystaniem wiedzy wypracowanej w ramach sieci unijnych ekspertów ds. bezpieczeństwa i zwalczania terroryzmu. Dobrym punktem odniesienia dla takiej ukierunkowanej współpracy jest wspólny plan działania dla Bałkanów Zachodnich w zakresie zwalczania terroryzmu. Dążyć należy w szczególności do wspierania zdolności krajów partnerskich w zakresie identyfikowania i lokalizowania zagranicznych bojowników terrorystycznych. UE będzie również nadal propagować wielostronną współpracę, współpracując z głównymi światowymi podmiotami w tej dziedzinie, takimi jak ONZ, NATO, Rada Europy, Interpol i OBWE. Będzie też współpracować ze Światowym Forum na rzecz Zwalczania Terroryzmu i światową koalicją przeciwko Daiszowi, a także z odpowiednimi podmiotami społeczeństwa obywatelskiego. Ważną rolę we współdziałaniu z państwami trzecimi w zakresie zapobiegania terroryzmowi i piractwu odgrywają również instrumenty polityki zewnętrznej Unii, w tym w zakresie rozwoju i współpracy. Współpraca międzynarodowa jest też niezbędna w celu odcięcia wszelkich źródeł **finansowania terroryzmu**, na przykład za pośrednictwem Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy.

Przestępczość zorganizowana

[88] Taki właśnie charakter miały m.in. tragiczne w skutkach zamachy w Oslo (2011 r.), Paryżu (2015 r.), Brukseli (2016 r.) i Manchesterze (2017 r.). Materiały wybuchowe domowej roboty wykorzystano również w zamachu w Lyonie (2019 r.), w którym rannych zostało 13 osób.

[89] W tym nowych kompetencji Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex).

[90] W konkluzjach Rady z dnia 16 czerwca 2020 r. podkreślono potrzebę ochrony obywateli UE przed terroryzmem i brutalnym ekstremizmem pod wszelkimi postaciami, niezależnie od ich pochodzenia, a także potrzebę dalszego wzmacniania zewnętrznego zaangażowania UE w zwalczanie terroryzmu i działań w niektórych priorytetowych obszarach geograficznych i tematycznych.

Przestępczość zorganizowana pociąga za sobą ogromne koszty ekonomiczne i ludzkie. Szacuje się, że straty gospodarcze spowodowane przestępczością zorganizowaną i korupcją wynoszą od 218 do 282 mld EUR rocznie[91]. W 2017 r. w Europie prowadzono dochodzenia w sprawie ponad 5 000 zorganizowanych grup przestępczych – o 50 % więcej niż w 2013 r.[92] Przestępczość zorganizowana w coraz większym stopniu prowadzona jest transgranicznie, m.in. z bezpośredniego sąsiedztwa UE, co wskazuje na konieczność zintensyfikowanej współpracy operacyjnej i wymiany informacji z partnerami w sąsiedztwie.

Pojawiają się nowe wyzwania, a przestępstw coraz częściej dokonuje się w internecie: podczas pandemii COVID-19 odnotowano ogromny wzrost skali oszustw internetowych na szkodę szczególnie wrażliwych grup społecznych, a także kradzieże (m.in. z włamaniem) wyrobów zdrowotnych i sanitarnych[93]. UE musi intensywniej przeciwdziałać przestępczości zorganizowanej, w tym na szczeblu międzynarodowym, przy użyciu większej liczby narzędzi pozwalających na rozbicie przestępczych modeli biznesowych. Zwalczanie przestępczości zorganizowanej wymaga również ścisłej współpracy z organami administracji lokalnej i regionalnej oraz ze społeczeństwem obywatelskim – są to kluczowi partnerzy w zapobieganiu przestępczości oraz w udzielaniu pomocy i wsparcia ofiarom. Szczególnie istotne są w tym kontekście potrzeby administracji w regionach przygranicznych. Działania w tym zakresie zostaną połączone w **agendę na rzecz zwalczania przestępczości zorganizowanej**.

Ponad jedna trzecia zorganizowanych grup przestępczych działających w UE zajmuje się produkcją i dystrybucją środków odurzających lub handlem tymi środkami. Uzależnienie od narkotyków doprowadziło w UE w 2019 r. do ponad ośmiu tysięcy zgonów w wyniku przedawkowania. Większość **handlu narkotykami** odbywa się transgranicznie, a duża część zysków z niego przenika do legalnej gospodarki[94]. Nowa agenda antynarkotykowa UE[95] przewiduje intensywniejsze działania Unii i państw członkowskich w zakresie ograniczania zarówno popytu na środki odurzające, jak i ich podaży. Określono w niej wspólne działania służące rozwiązaniu wspólnego problemu, a także przewidziano zacieśnienie dialogu i współpracy między UE a partnerami zewnętrznymi w kwestiach związanych z narkotykami. W oparciu o wyniki oceny Europejskiego Centrum Monitorowania Narkotyków i Narkomanii Komisja rozważy, czy jego mandat wymaga aktualizacji w celu sprostania nowym wyzwaniom.

Zorganizowane grupy przestępcze i terroryści odgrywają również kluczową rolę w handlu **nielegalną bronią palną**. W latach 2009–2018 w Europie doszło do 23 masowych strzelanin, w których zginęło ponad 340 osób[96]. Broń palna często trafia do Unii za pośrednictwem krajów jej bezpośredniego sąsiedztwa[97]. Wskazuje to na potrzebę

---

[91] W odniesieniu do produktu krajowego brutto (PKB); sprawozdanie Europolu: „Does crime still pay? – Criminal asset recovery in the EU" [„Czy przestępstwo nadal popłaca? Odzyskiwanie mienia pochodzącego z działalności przestępczej w UE"], 2016 r.

[92] Europol, Serious and Organised Threat Assessments (SOCTA) [Oceny zagrożenia przestępczością zorganizowaną], 2013 i 2017 r.

[93] Europol, 2020 r.

[94] „EMCDDA and Europol EU Drugs Market Report 2019" [„Sprawozdanie EMCDDA i Europolu na temat rynku środków odurzających w UE w 2019 r."] (listopad 2019 r.)

[95] Agenda i plan działania UE w zakresie narkotyków na lata 2021–2025, COM(2020) 606.

[96] Flamandzki Instytut Pokoju, „Armed to kill" [„Uzbrojeni, by zabijać"] (październik 2019 r.).

[97] Od 2002 r. UE udostępnia środki na zwalczanie rozprzestrzeniania broni strzeleckiej i lekkiej oraz handlu nią w tym regionie, m.in. finansując sieć ekspertów ds. broni palnej w krajach Europy Południowo-Wschodniej (SEEFEN). Od 2019 r. partnerzy z Bałkanów Zachodnich są w pełni zaangażowani

wzmocnienia koordynacji i współpracy zarówno w ramach UE, jak i z partnerami międzynarodowymi, w szczególności z Interpolem, w celu harmonizacji gromadzenia informacji i sprawozdawczości w zakresie konfiskat broni. Zasadnicze znaczenie ma również poprawa zdolności śledzenia poszczególnych sztuk broni, m.in. w internecie, oraz zapewnienie wymiany informacji między organami wydającymi zezwolenia a organami ścigania. Komisja przedstawia nowy **plan działania UE przeciwko nielegalnemu handlowi bronią palną**[98]. Oceni również, czy przepisy dotyczące zezwoleń na wywóz oraz środki w zakresie przywozu i tranzytu broni nadal spełniają swoje zadanie[99].

Organizacje przestępcze traktują migrantów i osoby potrzebujące ochrony międzynarodowej jak towar. 90 % migrantów przybywających nielegalnie do UE korzysta w tym celu z usług siatek przestępczych[100]. Przemyt migrantów jest również często powiązany z innymi formami przestępczości zorganizowanej, w szczególności z handlem ludźmi[101]. Ten zaś proceder nie tylko generuje ogromne koszty ludzkie, lecz pociąga za sobą inne formy wykorzystywania ludzi, które przynoszą przestępcom w skali światowej roczny zysk szacowany przez Europol na 29,4 mld EUR. Jest to przestępstwo transgraniczne, wykorzystujące popyt zarówno wewnątrz, jak i poza UE, i ma wpływ na wszystkie państwa członkowskie UE. Dotychczasowa niska skuteczność w zakresie wykrywania tych przestępstw oraz ścigania i skazywania ich sprawców wskazuje na konieczność zastosowania nowego, usprawnionego podejścia. Nowe **kompleksowe podejście do problemu handlu ludźmi** pozwoli na powiązanie rozmaitych działań. Ponadto Komisja przedstawi **nowy unijny plan działania na rzecz zwalczania przemytu migrantów** na lata 2021–2025. Działania w obu tych dziedzinach będą koncentrować się na zwalczaniu siatek przestępczych, intensywniejszej współpracy i wspieraniu działań w zakresie egzekwowania prawa.

Zorganizowane grupy przestępcze, a także terroryści, poszukują również możliwości działania w innych dziedzinach, zwłaszcza tam, gdzie można liczyć na wysokie zyski, a wykrywalność przestępstw jest niska. Jedną z takich dziedzin są **przestępstwa przeciwko środowisku**. Nielegalne działania w zakresie polowań i handlu dziką fauną i florą, wydobycia surowców, pozyskiwania drewna oraz składowania i przemieszczania odpadów stały się czwartym co do wielkości rodzajem działalności przestępczej w skali świata[102]. Do celów przestępczych bywają również wykorzystywane systemy handlu uprawnieniami do emisji i świadectw energetycznych, a także środki finansowe przeznaczone na budowanie odporności środowiskowej i zrównoważony rozwój. Oprócz wspierania intensywniejszych działań podejmowanych przez UE, państwa członkowskie i społeczność międzynarodową na rzecz walki z przestępstwami przeciwko środowisku[103], Komisja ocenia obecnie, czy dyrektywa w sprawie przestępstw przeciwko środowisku[104] nadal spełnia swoje zadanie. Jedną z najbardziej dochodowych form działalności przestępczej stał się również **nielegalny**

---

w priorytetowe działania związane z bronią palną w ramach europejskiej multidyscyplinarnej platformy przeciwko zagrożeniom przestępstwami (EMPACT).

98 COM(2020) 608.

99 Rozporządzenie (UE) nr 258/2012 wdrażające art. 10 Protokołu Narodów Zjednoczonych przeciwko nielegalnemu wytwarzaniu i obrotowi bronią palną.

100 Źródło: Europol.

101 Europol, Europejskie Centrum Zwalczania Przemytu Migrantów, 4. sprawozdanie roczne.

102 UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime [Ocena szybkiego reagowania UNEP-INTERPOL – Wzrost skali przestępstw przeciwko środowisku], czerwiec 2016 r.

103 Zob. Europejski Zielony Ład, COM(2019) 640 final.

104 Dyrektywa Parlamentu Europejskiego i Rady 2008/99/WE w sprawie ochrony środowiska poprzez prawo karne.

handel dobrami kultury. Jest on źródłem finansowania terroryzmu i przestępczości zorganizowanej, a jego skala rośnie. Należy rozważyć dostępne sposoby skuteczniejszego śledzenia dóbr kultury w internecie i poza nim na rynku wewnętrznym, a także możliwości współpracy z państwami trzecimi, w których dokonuje się ich rabunku. Aktywnego wsparcia wymagają też organy ścigania i środowiska akademickie.

Przestępstwa gospodarcze i finansowe są bardzo złożone, ale ich skutki dotykają w UE każdego roku milionów obywateli i tysiące przedsiębiorstw. Zwalczanie oszustw ma kluczowe znaczenie i wymaga działań na szczeblu UE. Europol wraz z Eurojustem, Prokuraturą Europejską i Europejskim Urzędem ds. Zwalczania Nadużyć Finansowych wspiera państwa członkowskie i UE w ochronie rynków gospodarczych i finansowych oraz pieniędzy podatników UE. Prokuratura Europejska w pełni rozpocznie działanie pod koniec 2020 r. i będzie prowadzić dochodzenia w sprawach przestępstw przeciwko budżetowi UE, m.in. nadużyć finansowych, korupcji i prania pieniędzy, ścigając i stawiając przed sądem ich sprawców. Będzie również zajmować się transgranicznymi oszustwami związanymi z VAT, które kosztują podatników co najmniej 50 mld EUR rocznie.

Komisja będzie także wspierać rozwój wiedzy specjalistycznej i ram prawnych w odniesieniu do nowych zagrożeń, związanych np. z kryptoaktywami czy nowymi systemami płatności. Komisja rozważy w szczególności reakcję na pojawienie się kryptoaktywów takich jak bitcoin, analizując spodziewany wpływ tych nowych technologii na sposób emisji, obiegu i udostępniania aktywów finansowych oraz dostępu do nich.

W Unii Europejskiej powinna obowiązywać zasada zerowej tolerancji wobec nielegalnych pieniędzy. W ciągu trzydziestu lat UE wypracowała solidne ramy regulacyjne w zakresie zapobiegania **praniu pieniędzy** i finansowaniu terroryzmu oraz zwalczania tych zjawisk, przy pełnym poszanowaniu potrzeby ochrony danych osobowych. Rośnie jednak zgoda co do tego, że wdrażanie obecnych ram wymaga znacznej poprawy. Należy rozwiązać problem daleko idących rozbieżności w sposobie stosowania tych ramowych przepisów i poważnych niedociągnięć w ich egzekwowaniu. Jak określono w planie działania z maja 2020 r.[105], trwają prace nad oceną możliwości wzmocnienia unijnych ram przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Obszary, które należy zbadać, obejmują wzajemne połączenie krajowych scentralizowanych rejestrów rachunków bankowych, co mogłoby znacznie przyspieszyć dostęp do informacji finansowych dla jednostek analityki finansowej i właściwych organów.

Zyski zorganizowanych grup przestępczych w UE szacuje się na 110 mld EUR rocznie. Prowadzone obecnie działania w celu ich zwalczania to m.in. zharmonizowane przepisy dotyczące konfiskaty i odzyskiwania mienia[106], mające służyć skuteczniejszemu zabezpieczaniu i zajmowaniu mienia pochodzącego z działalności przestępczej w UE oraz sprzyjać wzajemnemu zaufaniu i skutecznej współpracy transgranicznej między państwami członkowskimi. Niemniej jednak tylko około 1 % tych zysków udaje się konfiskować[107], przez co zorganizowane grupy przestępcze mogą inwestować w rozwój działalności i przenikać do legalnej gospodarki. Do prania pieniędzy wykorzystywane są zwłaszcza małe i średnie przedsiębiorstwa, którym niejednokrotnie trudno uzyskać kredyt. Komisja przeanalizuje wdrożenie prawodawstwa[108] i ewentualną potrzebę wprowadzenia dalszych

[105] Plan działania na rzecz zapobiegania praniu pieniędzy i finansowaniu terroryzmu, C(2020) 2800.

[106] Przepisy UE wymagają utworzenia biur ds. odzyskiwania mienia we wszystkich państwach członkowskich.

[107] Sprawozdanie pt. „Odzyskiwanie i konfiskata mienia: Przestępstwa nigdy nie mogą się opłacać”, COM(2020) 217 final.

[108] Dyrektywa 2014/42/UE w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa.

wspólnych przepisów, w tym dotyczących konfiskaty bez uprzedniego wyroku skazującego. Biura ds. odzyskiwania mienia[109], odgrywające w tym procesie kluczową rolę, mogłyby być również wyposażone w lepsze narzędzia pozwalające na sprawniejsze identyfikowanie i śledzenie aktywów w całej UE oraz poprawę wskaźników ich konfiskaty.

Z przestępczością zorganizowaną silnie powiązana jest **korupcja**. Jak ocenia się w dużym przybliżeniu, samo to zjawisko kosztuje gospodarkę UE 120 mld EUR rocznie[110]. Zapobieganie korupcji i jej zwalczanie będą nadal przedmiotem regularnego monitorowania w ramach mechanizmu praworządności oraz europejskiego semestru. W kontekście europejskiego semestru przeanalizowano wyzwania w zakresie zwalczania korupcji m.in. w zamówieniach publicznych, administracji publicznej, otoczeniu działalności gospodarczej czy opiece zdrowotnej. Kwestia zwalczania korupcji znajdzie się w nowym corocznym sprawozdaniu Komisji na temat praworządności, co umożliwi prowadzenie dialogu zapobiegawczego z władzami krajowymi i zainteresowanymi stronami na szczeblu unijnym i krajowym. Również organizacje społeczeństwa obywatelskiego mogą odegrać znaczącą rolę w stymulowaniu działań władz publicznych w zakresie zapobiegania i przeciwdziałania przestępczości zorganizowanej i korupcji; użyteczne byłoby stworzenie wspólnego forum dla tych grup. Ze względu na transgraniczny charakter przestępczości zorganizowanej i korupcji kolejnym kluczowym wymiarem jest współpraca z regionami sąsiadującymi z UE i wzajemna pomoc w zwalczaniu tych zjawisk.

Główne działania
• Agenda antyterrorystyczna dla UE, obejmująca nowe sposoby przeciwdziałania radykalizacji postaw w UE • Nowe działania antyterrorystyczne podejmowane wspólnie z kluczowymi państwami trzecimi i organizacjami międzynarodowymi • Agenda na rzecz zwalczania przestępczości zorganizowanej, w tym handlu ludźmi • Agenda i plan działania UE w zakresie narkotyków na lata 2021–2025 • Ocena działania Europejskiego Centrum Monitorowania Narkotyków i Narkomanii • Plan działania UE w sprawie nielegalnego handlu bronią palną na lata 2020–2025 • Przegląd przepisów w sprawie zabezpieczenia i konfiskaty mienia oraz biur ds. odzyskiwania mienia • Ocena dyrektywy o przestępstwach przeciwko środowisku • Unijny plan działania na rzecz zwalczania przemytu migrantów na lata 2021–2025

4. Silny europejski ekosystem bezpieczeństwa

Rzeczywista i skuteczna unia bezpieczeństwa musi być wspólnym przedsięwzięciem wszystkich grup społecznych. Uczestniczyć w nim muszą rządy, organy ścigania, sektor prywatny, system oświaty i szkolnictwa i sami obywatele. Należy zapewnić im odpowiednie narzędzia i wzajemne połączenia w celu budowania gotowości i odporności dla wszystkich, w szczególności osób w najtrudniejszej sytuacji, ofiar oraz świadków.

[109] Decyzja Rady 2007/845/WSiSW dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem.

[110] Oszacowanie całkowitych kosztów gospodarczych korupcji jest trudne, lecz próby takie, podejmowane przez rozmaite organy, m.in. Międzynarodową Izbę Handlową, Transparency International, inicjatywę ONZ Global Compact oraz Światowe Forum Ekonomiczne, wskazują, że skala korupcji odpowiada 5 % światowego PKB.

We wszystkich strategiach politycznych należy uwzględnić wymiar bezpieczeństwa. UE może przyczynić się do tego na każdym szczeblu. W gospodarstwach domowych przemoc w rodzinie stanowi jedno z najpoważniejszych zagrożeń bezpieczeństwa. 22 % kobiet w UE doświadczyło przemocy ze strony partnera życiowego[111]. Przystąpienie UE do konwencji stambulskiej o zapobieganiu i zwalczaniu przemocy wobec kobiet i przemocy domowej jest w dalszym ciągu priorytetem. Jeżeli nie dojdzie do przełomu w negocjacjach, Komisja podejmie inne działania, aby osiągnąć te same cele, które są realizowane w ramach konwencji, w tym zaproponuje dodanie przemocy wobec kobiet do wykazu przestępstw UE określonych w Traktacie.

Współpraca i wymiana informacji

Jednym z najważniejszych sposobów, w jaki UE może przyczynić się do ochrony obywateli, jest ułatwianie skutecznej współpracy podmiotów odpowiedzialnych za bezpieczeństwo. Współpraca i wymiana informacji to najpotężniejsze narzędzia do walki z przestępczością i terroryzmem oraz dążenia do sprawiedliwości. Aby były one skuteczne, muszą być ukierunkowane i odbywać się w odpowiednim czasie. Aby budziły zaufanie, należy z nich korzystać, przestrzegając wspólnych zabezpieczeń i środków kontroli.

W celu dalszego rozwijania **współpracy operacyjnej** między państwami członkowskimi **w zakresie ścigania przestępstw** ustanowiono szereg unijnych instrumentów i strategii dotyczących określonych sektorów i dziedzin[112]. Jednym z głównych instrumentów UE służących wspieraniu współpracy między państwami członkowskimi w zakresie ścigania przestępstw jest System Informacyjny Schengen, wykorzystywany do wymiany danych na temat poszukiwanych i zaginionych osób i przedmiotów w czasie rzeczywistym. Rezultaty jego wykorzystania są odczuwalne w postaci aresztowań przestępców, konfiskat narkotyków i w liczbie uratowanych potencjalnych ofiar[113]. Współpracę tę można jednak jeszcze dodatkowo zacieśnić dzięki usprawnieniu i modernizacji dostępnych instrumentów. Większość ram prawnych UE leżących u podstaw współpracy operacyjnej w zakresie ścigania przestępstw została opracowana 30 lat temu. Złożona sieć umów dwustronnych między państwami członkowskimi, często przestarzałych lub niedostatecznie wykorzystywanych, grozi fragmentacją. W mniejszych lub śródlądowych państwach funkcjonariusze organów ścigania, którzy pracują ponad granicami, muszą prowadzić działania operacyjne na podstawie różnych (w niektórych przypadkach nawet do siedmiu) zbiorów przepisów; w rezultacie niektóre operacje, np. pościgi transgraniczne podejrzanych z przekroczeniem granic wewnętrznych, po prostu się nie odbywają. Współpraca operacyjna w zakresie nowych technologii, takich jak drony, również nie jest objęta obecnymi ramami UE.

Specjalna współpraca w zakresie ścigania przestępstw, która może również pomóc w zapewnieniu kluczowego wsparcia w odniesieniu do innych celów politycznych, takich jak zapewnienie wkładu w zakresie bezpieczeństwa na potrzeby nowej oceny bezpośrednich inwestycji zagranicznych, może przyczyniać się do zwiększenia skuteczności operacyjnej. Komisja zbada, jak może w tym pomóc kodeks współpracy policyjnej. Organy ścigania państw członkowskich w coraz większym stopniu korzystają ze wsparcia i wiedzy fachowej na szczeblu UE, natomiast Centrum Analiz Wywiadowczych UE (INTCEN) odgrywa kluczową rolę w propagowaniu wymiany informacji strategicznych między służbami

[111] Unia równości: strategia na rzecz równouprawnienia płci na lata 2020–2025, COM(2020) 152.

[112] Na przykład plan działania w ramach strategii UE w zakresie bezpieczeństwa morskiego, dzięki któremu osiągnięto ważne postępy we współpracy pomiędzy agencjami UE w zakresie funkcji straży przybrzeżnej.

[113] Walka UE z przestępczością zorganizowaną w 2019 r. (Rada, 2020 r.).

wywiadowczymi i służbami bezpieczeństwa państw członkowskich, umożliwiając w ten sposób instytucjom UE orientację sytuacyjną w zakresie danych wywiadowczych[114]. **Europol** może również odgrywać kluczową rolę w rozwijaniu współpracy z państwami trzecimi w celu zwalczania przestępczości i terroryzmu zgodnie z innymi politykami i narzędziami zewnętrznymi UE. Europol zmaga się jednak obecnie z wieloma poważnymi ograniczeniami, zwłaszcza w odniesieniu do bezpośredniej wymiany danych osobowych z podmiotami prywatnymi, co utrudnia mu skuteczne wspieranie państw członkowskich w zwalczaniu terroryzmu i przestępczości. Obecnie trwa ocena kompetencji Europolu w celu zweryfikowania, w jaki sposób można je poprawić, by Urząd mógł w pełni wykonywać swoje zadania. W tym kontekście właściwe organy na szczeblu UE (takie jak OLAF, Europol, Eurojust i Prokuratura Europejska) powinny również ściślej współpracować i usprawniać wymianę informacji.

Kolejnym kluczowym elementem łączącym jest dalszy rozwój **Eurojustu**, tak aby zmaksymalizować synergię między współpracą organów ścigania a współpracą sądową. UE odniosłaby korzyści również dzięki większej spójności strategicznej: **EMPACT**[115], cykl polityki UE dotyczącej poważnej i międzynarodowej zorganizowanej przestępczości, zapewnia organom metodykę opartą na danych wywiadowczych dotyczących przestępczości w celu wspólnego zwalczania najważniejszych zagrożeń przestępstwami mających wpływ na UE. W ostatnim dziesięcioleciu doprowadziło to do uzyskania istotnych rezultatów operacyjnych[116]. W oparciu o doświadczenia praktyków należy usprawnić i uprościć istniejący mechanizm, aby lepiej reagować na najbardziej palące i zmieniające się zagrożenia przestępstwami w kontekście nowego cyklu polityki na lata 2022–2025.

Terminowe i odpowiednie **informacje** mają kluczowe znaczenie w codziennej pracy organów ścigania. Pomimo opracowania nowych baz danych na szczeblu UE w zakresie bezpieczeństwa i zarządzania granicami wiele informacji nadal znajduje się w krajowych bazach danych lub jest wymienianych bez użycia tych narzędzi. Skutkiem tego jest znaczne dodatkowe obciążenie pracą, opóźnienia i zwiększone ryzyko przeoczenia kluczowych informacji. Sprawniejsze, szybsze i uproszczone procedury, obejmujące całą wspólnotę bezpieczeństwa, przyniosłyby lepsze rezultaty. Odpowiednie narzędzia są niezbędne, by do skutecznego ścigania przestępstw można wykorzystać potencjał wymiany informacji, przy zachowaniu niezbędnych zabezpieczeń, tak aby udostępnianie danych odbywało się z poszanowaniem przepisów o ochronie danych i praw podstawowych. W świetle zmian w zakresie technologii, kryminalistyki i ochrony danych oraz zmieniających się potrzeb operacyjnych UE mogłaby rozważyć, czy istnieje potrzeba unowocześnienia instrumentów, takich jak **decyzje w sprawie konwencji z Prüm z 2008 r.**, ustanawiających automatyczną wymianę danych dotyczących DNA, odcisków palców i danych rejestracyjnych pojazdów, aby umożliwić zautomatyzowaną wymianę dodatkowych kategorii danych, które są już dostępne w bazach danych o przestępstwach lub innych bazach danych państw członkowskich, do celów postępowań przygotowawczych. Ponadto Komisja zbada możliwość wymiany informacji z akt policyjnych w celu ustalenia, czy w innych państwach członkowskich istnieją takie informacje dotyczące danej osoby, oraz ułatwienia dostępu do nich po ich zidentyfikowaniu, przy zachowaniu niezbędnych zabezpieczeń.

Informacje na temat podróżnych przyczyniły się do usprawnienia kontroli granicznych, ograniczenia nielegalnej migracji oraz zidentyfikowania osób stwarzających ryzyko dla

[114] INTCEN jako jedyna platforma umożliwia służbom wywiadowczym i służbom bezpieczeństwa państw członkowskich zapewnianie UE orientacji sytuacyjnej na podstawie danych wywiadowczych.

[115] EMPACT – Europejska multidyscyplinarna platforma przeciwko zagrożeniom przestępstwami.

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

bezpieczeństwa. Dane pasażera przekazywane przed podróżą to dane biograficzne każdego pasażera pobierane przez przewoźników lotniczych podczas odprawy i przesyłane z wyprzedzeniem do organów kontroli granicznej w miejscu przeznaczenia. Przegląd ram prawnych[117] mógłby umożliwić skuteczniejsze wykorzystanie informacji przy jednoczesnym zapewnieniu zgodności z przepisami o ochronie danych i ułatwieniu przepływu pasażerów. Dane dotyczące przelotu pasażera (dane PNR) to dane dostarczane przez pasażerów podczas rezerwacji lotów. Wdrożenie dyrektywy w sprawie danych dotyczących przelotu pasażera[118] ma zasadnicze znaczenie; Komisja będzie je w dalszym ciągu wspierać i egzekwować. Ponadto w ramach działań w perspektywie średniookresowej Komisja rozpocznie przegląd obecnego podejścia do **przekazywania danych PNR do państw trzecich**.

Współpraca sądowa jest niezbędnym uzupełnieniem działań policji mających na celu zwalczanie przestępczości transgranicznej. W ciągu ostatnich 20 lat we współpracy sądowej zaszły poważniejsze zmiany. Organy takie jak **Prokuratura Europejska** i **Eurojust** muszą dysponować środkami niezbędnymi do działania w pełnym zakresie lub do zapewnienia ich wzmocnienia. Można również zacieśnić współpracę między przedstawicielami zawodów prawniczych poprzez podjęcie dalszych kroków na rzecz wzajemnego uznawania orzeczeń sądowych, szkoleń kadr wymiaru sprawiedliwości i wymiany informacji. Celem powinno być zwiększenie wzajemnego zaufania między sędziami i prokuratorami, co ma kluczowe znaczenie dla sprawnego prowadzenia postępowań transgranicznych. Wykorzystanie **technologii cyfrowych** również może poprawić skuteczność naszych systemów wymiaru sprawiedliwości. Tworzony jest nowy system wymiany cyfrowej służący przekazywaniu europejskich nakazów dochodzeniowych, wniosków o wzajemną pomoc prawną oraz powiązanych komunikatów między państwami członkowskimi, przy wsparciu Eurojustu. Komisja będzie współpracować z państwami członkowskimi nad przyspieszeniem wdrożenia niezbędnych systemów informatycznych na szczeblu krajowym.

Współpraca międzynarodowa jest również kluczowa dla skutecznego ścigania przestępstw i współpracy sądowej. Umowy dwustronne z najważniejszymi partnerami odgrywają zasadniczą rolę w zabezpieczaniu informacji i dowodów spoza UE. Istotna jest rola **Interpolu**, jednej z największych międzyrządowych organizacji policji kryminalnej. Komisja przeanalizuje możliwe sposoby zacieśnienia współpracy z Interpolem, w tym ewentualny dostęp do baz danych Interpolu oraz wzmocnienie współpracy operacyjnej i strategicznej. Organy ścigania w UE polegają również na najważniejszych krajach partnerskich, jeśli chodzi o identyfikację i ściganie przestępców i terrorystów. **Partnerstwa na rzecz bezpieczeństwa między UE a państwami trzecimi** mogłyby zostać wzmocnione w celu zacieśnienia współpracy służącej zwalczaniu wspólnych zagrożeń, takich jak terroryzm, przestępczość zorganizowana, cyberprzestępczość, niegodziwe traktowanie dzieci w celach seksualnych oraz handel ludźmi. Takie podejście, które czerpie z ugruntowanej współpracy i dialogów na temat bezpieczeństwa, opierałoby się na wspólnych interesach w obszarze bezpieczeństwa.

Podobnie jak wymiana informacji, wymiana wiedzy fachowej może mieć szczególne znaczenie w zwiększaniu gotowości organów ścigania do reagowania na **zagrożenia nietradycyjne**. Oprócz zachęcania do wymiany najlepszych praktyk Komisja zbada

[117] Dyrektywa Rady 2004/82/WE w sprawie zobowiązania przewoźników do przekazywania danych pasażerów.

[118] Dyrektywa 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

możliwość wprowadzenia **mechanizmu koordynacji działań sił policyjnych na szczeblu UE** w przypadku wystąpienia zdarzeń spowodowanych działaniem siły wyższej, takich jak pandemie. Pandemia udowodniła również, że podstawowe znaczenie w walce z przestępczością i terroryzmem będzie miała współpraca policji ze społecznością lokalną w formie cyfrowej, której to współpracy towarzyszą ramy prawne ułatwiające działania policji w internecie. Dzięki partnerstwom między policją a społecznością lokalną, w internecie i poza nim, można zapobiegać przestępstwom oraz łagodzić skutki przestępczości zorganizowanej, radykalizacji postaw i działalności terrorystycznej. Połączenie rozwiązań stosowanych przez policję na szczeblu lokalnym z rozwiązaniami poziomu regionalnego, krajowego i unijnego stanowi najważniejszy czynnik decydujący o powodzeniu unii bezpieczeństwa UE.

Znaczenie silnych granic zewnętrznych

Nowoczesne i skuteczne zarządzanie granicami zewnętrznymi niesie za sobą podwójne korzyści: utrzymanie integralności strefy Schengen i zapewnienie bezpieczeństwa naszym obywatelom. Zaangażowanie wszystkich zainteresowanych stron na rzecz jak najlepszego zabezpieczania granicy może mieć rzeczywisty wpływ na zapobieganie przestępczości transgranicznej i terroryzmowi. Wspólne działania operacyjne w ramach niedawno wzmocnionej Europejskiej Straży Granicznej i Przybrzeżnej[119] przyczyniają się do wykrywania przestępczości transgranicznej i zapobiegania jej na **granicach zewnętrznych** i poza granicami UE. Działania celne w zakresie wykrywania zagrożeń dla ochrony i bezpieczeństwa w odniesieniu do wszystkich towarów przed ich przybyciem do UE oraz w zakresie kontroli towarów w momencie ich przybycia mają kluczowe znaczenie w walce z przestępczością transgraniczną i terroryzmem. W przyszłym planie działania w dziedzinie unii celnej przedstawione zostaną działania mające na celu również wzmocnienie zarządzania ryzykiem i zwiększenie bezpieczeństwa wewnętrznego, w tym w szczególności poprzez ocenę możliwości powiązania odpowiednich systemów informacyjnych na potrzeby analizy ryzyka w zakresie bezpieczeństwa.

W maju 2019 r. przyjęto ramy **interoperacyjności między systemami informacyjnymi UE** w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. Ta nowa struktura ma za zadanie poprawić wydajność i skuteczność nowych lub zmodernizowanych systemów informacyjnych[120]. Dzięki niej funkcjonariusze organów ścigania i straży granicznej oraz urzędnicy zajmujący się migracją będą otrzymywać informacje szybciej i w sposób bardziej systematyczny. Pomoże ona w prawidłowej identyfikacji oszustw dotyczących tożsamości i przyczyni się do ich zwalczania. Aby tak się stało, wdrażanie interoperacyjności powinno być priorytetem zarówno na szczeblu politycznym, jak i technicznym. Ścisła współpraca między agencjami UE i wszystkimi państwami członkowskimi będzie miała zasadnicze znaczenie dla osiągnięcia celu, jakim jest pełna interoperacyjność do 2023 r.

Przestępstwo przeciwko wiarygodności dokumentów podróży uznaje się za jedno z najczęściej popełnianych przestępstw. Fałszowanie dokumentów podróży ułatwia nielegalne przemieszczanie się przestępców i terrorystów oraz odgrywa kluczową rolę

[119] W jej skład wchodzą Europejska Agencja Straży Granicznej i Przybrzeżnej (Frontex) oraz organy straży granicznej i straży przybrzeżnej państw członkowskich.

[120] Systemu wjazdu/wyjazdu (EES), europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), rozszerzonego europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS-TCN), Systemu Informacyjnego Schengen, wizowego systemu informacyjnego oraz przyszłego zaktualizowanego Eurodac.

w handlu ludźmi i handlu narkotykami[121]. Komisja zbada, w jaki sposób rozszerzyć zakres dotychczasowych prac nad normami bezpieczeństwa dotyczącymi dokumentów pobytowych i dokumentów podróży w UE, w tym poprzez transformację cyfrową. Od sierpnia 2021 r. państwa członkowskie rozpoczną wydawanie dokumentów tożsamości i dokumentów pobytowych zgodnie ze zharmonizowanymi normami bezpieczeństwa, obejmującymi chipy zawierające identyfikatory biometryczne, które mogą być weryfikowane przez wszystkie służby graniczne UE. Komisja będzie monitorować wdrażanie tych nowych przepisów, w tym stopniowe zastępowanie dokumentów obecnie znajdujących się w obiegu.

Udoskonalanie badań i innowacji w dziedzinie bezpieczeństwa

Prace mające na celu zapewnienie cyberbezpieczeństwa oraz zwalczanie przestępczości zorganizowanej, cyberprzestępczości i terroryzmu w dużym stopniu zależą od opracowania narzędzi na przyszłość, które pomogą w tworzeniu bezpieczniejszych i pewniejszych nowych technologii, sprostają wyzwaniom związanym z technologiami i będą wspierać działania organów ścigania. To z kolei zależy od prywatnych partnerów i sektorów przemysłu.

Innowacje należy postrzegać jako strategiczne narzędzie do przeciwdziałania obecnym zagrożeniom i przewidywania zarówno przyszłych zagrożeń, jak i przyszłych możliwości. Innowacyjne technologie mogą umożliwić stworzenie nowych narzędzi, które zapewnią pomoc organom ścigania i innym podmiotom w obszarze bezpieczeństwa. Analityka z wykorzystaniem sztucznej inteligencji i technologia dużych zbiorów danych mogłyby wykorzystywać obliczenia wielkiej skali, aby zapewnić lepsze wykrywanie i szybką i wszechstronną analizę[122]. Podstawowym warunkiem rozwoju niezawodnych technologii są zbiory danych wysokiej jakości, dostępne właściwym organom w celu szkolenia, testowania i zatwierdzania algorytmów[123]. Ogólnie rzecz biorąc, ryzyko zależności technologicznej jest obecnie duże – UE jest na przykład importerem netto produktów i usług z zakresu cyberbezpieczeństwa, co oznacza, że gospodarka i infrastruktura krytyczna ponoszą wszelkie tego konsekwencje. Aby wykorzystywać technologie oraz zapewnić ciągłość dostaw, również w przypadku niepożądanych zdarzeń i kryzysów, Europa musi być obecna i musi wykazywać stosowne zdolności w najważniejszych częściach odpowiednich łańcuchów wartości.

Badania, innowacje i rozwój technologiczny w UE dają możliwość uwzględnienia wymiaru bezpieczeństwa podczas opracowywania tych technologii i ich zastosowań. Istotnych bodźców może dostarczyć kolejna generacja unijnych wniosków o finansowanie[124]. W inicjatywach dotyczących europejskich przestrzeni danych i infrastruktury chmury obliczeniowej od początku uwzględnia się kwestie bezpieczeństwa. Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach

[121] Związek między przestępstwem przeciwko wiarygodności dokumentów a handlem ludźmi przedstawiono w Drugim sprawozdaniu z postępów w zwalczaniu handlu ludźmi, COM(2018) 777, oraz towarzyszącym mu dokumencie SWD(2018) 473 i Sprawozdaniu sytuacyjnym Europolu w sprawie handlu ludźmi w UE, z 2016 r.

[122] Powinno to opierać się na strategii Komisji dotyczącej sztucznej inteligencji.

[123] Europejska strategia w zakresie danych, COM(2020) 66 final.

[124] Wnioski Komisji w sprawie programu „Horyzont Europa”, Funduszu Bezpieczeństwa Wewnętrznego, Funduszu Zintegrowanego Zarządzania Granicami, programu EUInvest, Europejskiego Funduszu Rozwoju Regionalnego i programu „Cyfrowa Europa” będą wspierać opracowywanie i wdrażanie innowacyjnych technologii i rozwiązań w zakresie bezpieczeństwa w całym łańcuchu wartości w dziedzinie bezpieczeństwa.

Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji[125] mają za zadanie stworzyć skuteczną i wydajną strukturę służącą gromadzeniu i udostępnianiu zdolności i wyników w zakresie badań w dziedzinie cyberbezpieczeństwa. Unijny program kosmiczny realizuje usługi wspierające bezpieczeństwo UE, jej państw członkowskich i obywateli[126].

Dzięki ponad 600 rozpoczętym od 2007 r. projektom o łącznej wartości bliskiej 3 mld EUR badania w dziedzinie bezpieczeństwa finansowane przez UE są kluczowym instrumentem napędzającym rozwój technologii i wiedzy służących opracowywaniu rozwiązań w dziedzinie bezpieczeństwa. W ramach przeglądu kompetencji Europolu Komisja rozważy utworzenie **europejskiego centrum innowacji na rzecz bezpieczeństwa wewnętrznego**[127]. Jego zadaniem byłoby wypracowanie wspólnych rozwiązań w odniesieniu do wspólnych wyzwań i możliwości w dziedzinie bezpieczeństwa, których to rozwiązań państwa członkowskie mogą nie być w stanie zbadać samodzielnie. Współpraca ma zasadnicze znaczenie dla ukierunkowania inwestycji na osiągnięcie jak najlepszych rezultatów i dla rozwoju innowacyjnych technologii, co przynosi zarówno korzyści pod względem bezpieczeństwa, jak i korzyści ekonomiczne.

Rozwijanie umiejętności i zwiększanie świadomości

Świadomość kwestii bezpieczeństwa i nabywanie umiejętności radzenia sobie z potencjalnymi zagrożeniami są niezbędne do budowy bardziej odpornego społeczeństwa, w którym obywatele, przedsiębiorstwa i administracje będą lepiej przygotowani. Wyzwania związane z infrastrukturą informatyczną i systemami elektronicznymi ujawniły potrzebę zwiększenia naszych ludzkich zdolności w zakresie gotowości i reagowania w obszarze cyberbezpieczeństwa. Pandemia uwydatniła również znaczenie transformacji cyfrowej we wszystkich obszarach gospodarki i społeczeństwa UE.

Nawet **podstawowa wiedza z zakresu zagrożeń dla bezpieczeństwa** oraz sposobów ich zwalczania może mieć rzeczywisty wpływ na odporność społeczeństwa. Świadomość ryzyka związanego z cyberprzestępczością oraz konieczność ochrony przed nią mogą współdziałać z ochroną ze strony usługodawców na potrzeby przeciwdziałania cyberatakom. Informacje o ryzyku i zagrożeniach związanych z handlem narkotykami mogą utrudniać przestępcom udaną realizację ich planów. UE może stymulować rozpowszechnianie najlepszych praktyk, na przykład poprzez sieć centrów bezpieczniejszego internetu[128], i dbać o to, by takie cele były uwzględniane w jej własnych programach.

Przyszły Plan działania w dziedzinie edukacji cyfrowej powinien obejmować ukierunkowane środki na rzecz budowania umiejętności informatycznych w zakresie

[125] Wniosek z dnia 12 września 2018 r. dotyczący rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji, COM(2018) 630.

[126] Na przykład program Copernicus zapewnia usługi umożliwiające nadzór nad granicami zewnętrznymi UE oraz nadzór morski, który pomaga przeciwdziałać piractwu i przemytowi, a także zapewnia wspierającą infrastrukturę krytyczną. Po osiągnięciu pełnej operacyjności będzie to kluczowe narzędzie misji i operacji cywilnych i wojskowych.

[127] Współpracowałoby ono również z Europejską Agencją Straży Granicznej i Przybrzeżnej (EBCGA)/Fronteksem, Agencją Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL), Agencją Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) i Wspólnym Centrum Badawczym.

[128] Zob. www.betterinternetforkids.eu: portal centralny i krajowe centra bezpieczniejszego internetu są obecnie finansowane w ramach instrumentu „Łącząc Europę”/Telekomunikacja, a finansowanie w przyszłości zaproponowano w ramach programu „Cyfrowa Europa”.

bezpieczeństwa w całej ludności. Niedawno przyjęty program na rzecz umiejętności[129] wspiera zdobywanie umiejętności przez całe życie. Obejmuje on specjalne działania mające na celu zwiększenie liczby absolwentów takich kierunków, jak nauki przyrodnicze, technologia, inżynieria, sztuka i matematyka. Dziedziny te są przydatne w nowatorskich obszarach, takich jak cyberbezpieczeństwo. Dodatkowe działania finansowane w ramach programu „Cyfrowa Europa" umożliwią specjalistom dotrzymywanie kroku zmianom w zakresie zagrożeń dla bezpieczeństwa, a jednocześnie wypełnienie braków w tym obszarze na unijnym rynku pracy. Rezultatem ogólnym będzie umożliwienie obywatelom nabywania umiejętności pozwalających na radzenie sobie z zagrożeniami dla bezpieczeństwa, a przedsiębiorstwom – znalezienie specjalistów, których potrzebują w tej dziedzinie. W przyszłości europejska przestrzeń badawcza i europejski obszar edukacji również będą propagować kariery w obszarze nauk przyrodniczych, technologii, inżynierii, sztuki i matematyki.

Ponadto ważne jest, by **ofiary** miały możliwość korzystania z przysługujących im praw; muszą one otrzymywać niezbędną pomoc i wsparcie, z uwzględnieniem szczególnych okoliczności. Zwłaszcza w odniesieniu do mniejszości i najbardziej bezbronnych ofiar, takich jak dzieci lub kobiety, które padły ofiarą handlu ludźmi do celów wykorzystywania seksualnego lub były narażone na przemoc domową, konieczne są szczególne wysiłki[130].

Szczególną rolę odgrywają lepsze **umiejętności w zakresie ścigania przestępstw**. Obecne i nowe zagrożenia technologiczne wymagają większych inwestycji w podnoszenie umiejętności pracowników organów ścigania na jak najwcześniejszym etapie i przez cały okres ich kariery zawodowej. Podstawowym partnerem państw członkowskich w tym zadaniu jest CEPOL. Szkolenia w zakresie ścigania przestępstw związane z rasizmem i ksenofobią oraz – ogólniej – w zakresie praw obywatelskich muszą być zasadniczym elementem unijnej kultury bezpieczeństwa. Krajowe systemy wymiaru sprawiedliwości i ich pracownicy muszą być również przygotowani, aby umieć dostosować się do bezprecedensowych wyzwań i na nie reagować. Szkolenia mają w tym zakresie kluczowe znaczenie, bowiem umożliwiają organom w terenie wykorzystywanie wspomnianych narzędzi w sytuacji operacyjnej. Ponadto należy dołożyć wszelkich starań, aby wzmocnić uwzględnianie aspektu płci i zwiększyć udział kobiet w ściganiu przestępstw.

Główne działania
• Wzmocnienie kompetencji Europolu • Zbadanie możliwości stworzenia unijnego kodeksu współpracy policyjnej oraz koordynacji działań policji w czasach kryzysu • Wzmocnienie Eurojustu w celu powiązania organów sądowych i organów ścigania • Przegląd dyrektywy w sprawie danych pasażera przekazywanych przed podróżą • Komunikat w sprawie zewnętrznego wymiaru kwestii danych dotyczących przelotu pasażera • Zacieśnianie współpracy między UE a Interpolem • Ramy negocjacji z kluczowymi państwami trzecimi w sprawie wymiany informacji • Lepsze normy bezpieczeństwa w odniesieniu do dokumentów podróży • Wykorzystanie europejskiego centrum innowacji w dziedzinie bezpieczeństwa

[129] Europejski program na rzecz umiejętności służący zrównoważonej konkurencyjności, sprawiedliwości społecznej i odporności, COM(2020) 274 final.

[130] Zob. Strategia na rzecz równouprawnienia płci, COM(2020) 152; Strategia w zakresie praw ofiar, COM(2020) 258; oraz europejska strategia na rzecz lepszego internetu dla dzieci, COM(2012) 196.

wewnętrznego

V. Wnioski

W coraz bardziej niespokojnym świecie Unia Europejska jest nadal powszechnie postrzegana jako jedno z najbezpieczniejszych i najlepiej chronionych miejsc. Nie można jednak zakładać, że taki stan się utrzyma.

Nowa strategia w zakresie unii bezpieczeństwa tworzy podstawy ekosystemu bezpieczeństwa, który obejmuje całe społeczeństwo europejskie. U jej podstaw leży przekonanie, że bezpieczeństwo jest wspólną odpowiedzialnością. Dotyczy ono nas wszystkich. Wszystkie organy rządowe, przedsiębiorstwa, organizacje społeczne, instytucje i obywatele muszą wypełniać swoje obowiązki, aby nasze społeczeństwa były bezpieczniejsze.

Dzisiaj kwestie bezpieczeństwa należy rozpatrywać z dużo szerszej perspektywy niż miało to miejsce w przeszłości. Należy przezwyciężyć fałszywe rozróżnienia między bezpieczeństwem fizycznym i cyfrowym. Strategia Unii Europejskiej w zakresie bezpieczeństwa obejmuje całe spektrum potrzeb w dziedzinie bezpieczeństwa i koncentruje się na obszarach o największym znaczeniu dla bezpieczeństwa UE w nadchodzących latach. Uznaje się w niej również, że zagrożenia dla bezpieczeństwa nie respektują granic geograficznych, a bezpieczeństwo wewnętrzne i zewnętrzne są ze sobą powiązane w coraz większym stopniu[131]. W tym kontekście ważne będzie, aby UE współpracowała z międzynarodowymi partnerami na rzecz ochrony wszystkich obywateli UE i w celu zapewnienia ścisłej koordynacji z działaniami zewnętrznymi UE we wdrażaniu tej strategii.

Nasze bezpieczeństwo jest powiązane z naszymi podstawowymi wartościami. Wszystkie działania i inicjatywy proponowane w ramach tej strategii będą w pełni zgodne z prawami podstawowymi i europejskimi wartościami. Stanowią one podstawę naszego europejskiego stylu życia i muszą pozostać w centrum wszystkich naszych działań.

Komisja w pełni zdaje sobie sprawę z faktu, że miarą wszelkich strategii czy działań jest ich wdrożenie i realizacja. W związku z tym konieczny jest niestrudzony nacisk na właściwe wdrażanie i egzekwowanie istniejących i przyszłych przepisów. Będzie to monitorowane za pomocą regularnych sprawozdań dotyczących unii bezpieczeństwa, a Komisja będzie skrupulatnie informować Parlament Europejski, Radę i interesariuszy o wszelkich istotnych działaniach; będzie je także w te działania angażować. Komisja jest ponadto gotowa organizować wspólne debaty z instytucjami na temat strategii w zakresie unii bezpieczeństwa i w nich uczestniczyć, aby podsumowywać osiągnięte postępy przy jednoczesnej wspólnej analizie przyszłych wyzwań.

Komisja zwraca się do Parlamentu Europejskiego i Rady o zatwierdzenie niniejszej strategii w zakresie unii bezpieczeństwa jako podstawy współpracy i wspólnego działania w dziedzinie bezpieczeństwa w ciągu najbliższych pięciu lat.

[131] Zob. Globalna strategia UE