



KOMISJA
EUROPEJSKA

WYSOKI PRZEDSTAWICIEL UNII
DO SPRAW ZAGRANICZNYCH I
POLITYKI BEZPIECZEŃSTWA

Bruksela, dnia 16.12.2020 r.
JOIN(2020) 18 final

WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY

Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę

WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY

Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę

I. WPROWADZENIE: CYBERBEZPIECZNA TRANSFORMACJA CYFROWA W ZŁOŻONYM ŚRODOWISKU ZAGROŻEŃ

Cyberbezpieczeństwo stanowi integralny element bezpieczeństwa Europejczyków. Obywatele muszą mieć pewność, że gdy korzystają z urządzeń podłączonych do internetu lub z sieci elektroenergetycznych, udają się do banku, lecą samolotem, korzystają z usług administracji publicznej czy leżą w szpitalu, są chronieni przed cyberzagrożeniami. Gospodarka, demokracja i społeczeństwo UE bardziej niż kiedykolwiek polegają na bezpiecznych i niezawodnych narzędziach cyfrowych i łączności. Cyberbezpieczeństwo ma zatem zasadnicze znaczenie dla budowania odpornej, ekologicznej i cyfrowej Europy.

Transport, energia i zdrowie, telekomunikacja, finanse, bezpieczeństwo, procesy demokratyczne, sektor kosmiczny i obronny są w dużym stopniu uzależnione od sieci i systemów informatycznych, które są w coraz większym stopniu wzajemnie połączone. Współzależności międzysektorowe są bardzo silne, ponieważ sieci i systemy informatyczne muszą z kolei być stale zasilane energią elektryczną, aby mogły funkcjonować. Liczba urządzeń podłączonych do internetu już teraz przewyższa liczbę mieszkańców planety, a przewiduje się, że do 2025 r. wzrośnie ona do 25 mld¹; jedna czwarta tych urządzeń będzie znajdować się w Europie. Cyfryzacja modeli pracy nabrała tempa w związku z pandemią COVID-19, podczas której 40 % pracowników UE przeszło na pracę zdalną, co prawdopodobnie wywarło trwały wpływ na życie codzienne². Zwiększa to podatność na cyberataki³. W przedmiotach podłączonych do internetu, które trafiają do konsumentów, często występują stwierdzone podatności, co dodatkowo zwiększa powierzchnię ataku w ramach szkodliwych działań w cyberprzestrzeni⁴. Przemysł unijny podlega coraz większej cyfryzacji i jest coraz bardziej połączony; oznacza to również, że cyberataki mogą mieć znacznie większy wpływ na gałęzie przemysłu i ekosystemy niż kiedykolwiek wcześniej.

¹ Szacunki telekomunikacyjnego stowarzyszenia branżowego GSMA; <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf>). Według prognozy International Data Corporation liczba skomunikowanych urządzeń, sensorów i kamer sięgnie 42,6 mld; <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>

² Według badania przeprowadzonego w czerwcu 2020 r. 47 % liderów biznesu stwierdziło, że zamierza zezwolić pracownikom na pracę zdalną w pełnym wymiarze czasu pracy, nawet gdy powrót do biur stanie się możliwy; 82 % zamierzało pozwolić pracownikom na pracę zdalną przez część czasu; <https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time>.

³ https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

⁴ Mirai, jeden z przykładów najbardziej szkodliwego złośliwego oprogramowania w historii, stworzył botnety składające się z ponad 600 000 urządzeń, które zakłóciły działanie wielu ważnych stron internetowych w Europie i Stanach Zjednoczonych.

Krajobraz zagrożeń pogarszają napięcia geopolityczne dotyczące kwestii globalnego i otwartego internetu oraz kontroli nad technologią w całym łańcuchu dostaw⁵. W wyniku tych napięć coraz więcej państw wznosi granice cyfrowe. Ograniczenia dotyczące internetu i w internecie zagrażają globalnemu i otwartemu charakterowi cyberprzestrzeni, a także praworządności, prawom podstawowym, wolności i demokracji – podstawowym wartościom UE. Cyberprzestrzeń jest coraz częściej wykorzystywana do celów politycznych i ideologicznych, a wysoka polaryzacja na szczeblu międzynarodowym utrudnia skuteczny multilateralizm. Zagrożenia hybrydowe łączą kampanie dezinformacyjne z cyberatakami na infrastrukturę, procesy gospodarcze i instytucje demokratyczne, które mogą powodować szkody fizyczne, doprowadzać do uzyskania nielegalnego dostępu do danych osobowych, doprowadzać do kradzieży tajemnic przemysłowych lub państwowych, mogą zmniejszać poziom zaufania i osłabiać spójność społeczną. Działania te osłabiają bezpieczeństwo międzynarodowe i stabilność międzynarodową oraz zmniejszają korzyści, jakie cyberprzestrzeń stwarza dla rozwoju gospodarczego, społecznego i politycznego.

Ataki na infrastrukturę krytyczną stanowią poważne zagrożenie globalne⁶. Internet ma strukturę zdecentralizowaną, bez centralnego ośrodka, i zarządza nim wiele zainteresowanych stron. Skutecznie poradził sobie z gwałtownym wzrostem natężenia ruchu, będąc jednocześnie regularnym celem szkodliwych prób zakłócenia jego działania⁷. Jednocześnie w zakresie komunikacji i hostingu, aplikacji i danych rośnie zależność od podstawowych funkcji globalnego i otwartego internetu, takich jak system nazw domen (DNS), oraz podstawowych usług internetowych. Usługi te są w coraz większym stopniu skupione pod kontrolą kilku prywatnych przedsiębiorstw⁸. Sytuacja ta powoduje, że europejska gospodarka i europejskie społeczeństwo są narażone na wstrząsy geopolityczne lub techniczne, które oddziałują na najważniejsze elementy internetu lub na jedno z tych przedsiębiorstw lub większą ich liczbę. Wzrost korzystania z internetu i zmiany wzorców spowodowane pandemią jeszcze bardziej obnażyły słabość łańcuchów dostaw, które polegają na tej infrastrukturze cyfrowej.

Obawy dotyczące bezpieczeństwa stanowią główny czynnik zniechęcający do korzystania z usług online⁹. Około dwie piąte unijnych użytkowników napotyka problemy związane z bezpieczeństwem, a trzy piąte uważa, że nie jest w stanie uchronić się przed

⁵ Obejmuje to części elektroniczne, analitykę danych, chmurę, szybsze i bardziej inteligentne sieci 5G i sieci kolejnych generacji, szyfrowanie, sztuczną inteligencję (AI) oraz nowe modele obliczeniowe i modele zaufanego przetwarzania danych, takie jak łańcuch bloków, *cloud-to-edge* oraz kwantowe technologie obliczeniowe.

⁶ Światowe Forum Ekonomiczne, Global Risks Report 2020.

⁷ Według Organizacji Współpracy Gospodarczej i Rozwoju pandemia spowodowała wzrost ruchu internetowego o 60 %; <https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/>. Organ Europejskich Regulatorów Łączności Elektronicznej i Komisja regularnie publikują [sprawozdania](#) na temat stanu przepustowości internetu w trakcie obowiązywania ograniczeń w przemieszczaniu się w związku z koronawirusem. Według sprawozdania ENISA w trzecim kwartale 2019 r. odnotowano wzrost łącznej liczby ataków typu DDoS o 241 % w porównaniu z trzecim kwartałem 2018 r. Ataki typu DDoS przeprowadzane są na coraz większą skalę, przy czym największy atak w historii miał miejsce w lutym 2020 r. i wygenerował maksymalne natężenie ruchu na poziomie 2,3 terabitów na sekundę. Podczas „awarii CenturyLink” w sierpniu 2020 r. problem z routowaniem u amerykańskiego dostawcy usług internetowych spowodował spadek światowego ruchu w sieci o 3,5 %; <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service>

⁸ Internet Society, The Global Internet Report: Consolidation in the Internet Economy; <https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/>

⁹ https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

cyberprzestępczością¹⁰. W ciągu ostatnich trzech lat jedna trzecia z nich otrzymała oszukańcze wiadomości e-mail lub odebrała telefony z prośbą o podanie danych osobowych, ale 83 % nigdy nie zgłosiło cyberprzestępstwa. Jedno na osiem przedsiębiorstw padło ofiarą cyberataków¹¹. Ponad połowa służbowych i prywatnych komputerów osobistych, które raz zostały zainfekowane złośliwym oprogramowaniem, została ponownie zainfekowana w ciągu tego samego roku¹². Każdego roku setki milionów zapisów wyciekają w wyniku naruszeń ochrony danych; średni koszt naruszenia dla pojedynczego przedsiębiorstwa wzrósł w 2018 r. do ponad 3,5 mln EUR¹³. Skutków cyberataku często nie da się ograniczyć do odizolowanego obszaru i mogą one wywołać reakcje łańcuchowe w całej gospodarce i społeczeństwie, dotykając milionów osób¹⁴.

Dochodzenia w sprawie niemal wszystkich rodzajów przestępstw mają element cyfrowy. W 2019 r. odnotowano trzykrotny wzrost liczby incydentów w ujęciu rok do roku. Szacowana liczba nowych przypadków złośliwego oprogramowania – najczęstszej metody prowadzenia cyberataku – wynosi 700 mln¹⁵. Szacuje się, że w 2020 r. roczny koszt, jaki w związku z cyberprzestępczością ponosi gospodarka światowa, wyniesie 5,5 bln EUR, dwukrotnie więcej niż w 2015 r.¹⁶ Stanowi to największy przepływ majątku w historii, większy niż światowy handel narkotykami. W przypadku jednego poważnego incydentu – ataku za pomocą oprogramowania typu ransomware o nazwie „WannaCry” w 2017 r. – koszt dla gospodarki światowej oszacowano na ponad 6,5 mld EUR¹⁷.

Usługi cyfrowe i sektor finansowy są jednymi z najczęstszych celów cyberataków, podobnie jak sektor publiczny i wytwórczy, ale gotowość i świadomość w zakresie cyberbezpieczeństwa wśród przedsiębiorstw i osób prywatnych są nadal niskie¹⁸ i istnieje znaczny niedobór umiejętności z zakresu cyberbezpieczeństwa wśród pracowników¹⁹. W 2019 r. odnotowano blisko 450 cyberincydentów dotyczących

¹⁰ Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2020 r.; <https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020>; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

¹¹ Komunikat prasowy Eurostatu, „Zdecydowana większość unijnych przedsiębiorstw wprowadziła środki w zakresie bezpieczeństwa ICT”, 6/2020 – 13 stycznia 2020 r. „Cyberataki na infrastrukturę krytyczną stały się normą w takich sektorach jak energetyka, opieka zdrowotna i transport”; WEF, The Global Risks Report 2020.

¹² Źródło: Comparitech.

¹³ Sprawozdanie na temat rocznych kosztów naruszeń ochrony danych, 2020, Ponemon Institute, oraz w oparciu o analizę ilościową 524 naruszeń w 17 regionach geograficznych i 17 sektorach; <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

¹⁴ Sprawozdanie Wspólnego Centrum Badawczego (JRC), „Cyberbezpieczeństwo, nasza kotwica w cyberprzestrzeni”; <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor>

¹⁵ Źródło: AV-TEST, <https://www.av-test.org/en/statistics/malware/>

¹⁶ Wspólne Centrum Badawcze „Cyberbezpieczeństwo, nasza kotwica w cyberprzestrzeni”.

¹⁷ Źródło: Cyence.

¹⁸ Przedsiębiorstwa, w szczególności MŚP, nadal posiadają niewielką wiedzę na temat cyberkradzieży tajemnic handlowych. PwC, „Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets” [„Badanie dotyczące skali i wpływu szpiegostwa przemysłowego i kradzieży tajemnic handlowych w cyberprzestrzeni: sprawozdanie mające na celu upowszechnianie informacji o środkach służących zwalczaniu cyberkradzieży tajemnic przedsiębiorstwa i zapobieganiu takim cyberkradzieżom”], 2018.

¹⁹ Zob. ENISA Threat Landscape 2020 [„Krajobraz zagrożeń 2020”]. Zob. również sprawozdanie Verizon na temat dochodzeń w sprawie naruszeń ochrony danych 2020; <https://enterprise.verizon.com/resources/reports/dbir/>

europejskiej infrastruktury krytycznej, takiej jak infrastruktura finansowa i energetyczna²⁰. W czasie pandemii szczególnie mocno ucierpiały organizacje i pracownicy opieki zdrowotnej. Ponieważ związek technologii ze światem fizycznym staje się nierozrwalny, cyberataki zagrażają życiu i dobrostanowi osób najbardziej narażonych²¹. Ocenia się, że ponad dwie trzecie przedsiębiorstw, w szczególności MŚP, nie ma doświadczenia w dziedzinie cyberbezpieczeństwa, a przedsiębiorstwa europejskie postrzega się jako gorzej przygotowane niż przedsiębiorstwa w Azji i Ameryce²². Szacuje się, że w Europie 291 000 stanowisk specjalistów w dziedzinie cyberbezpieczeństwa pozostaje nieobsadzonych. Zatrudnianie i szkolenie ekspertów ds. cyberbezpieczeństwa to powolny proces, co naraża organizacje na zwiększone ryzyko w cyberprzestrzeni²³.

W UE brakuje zbiorowej orientacji sytuacyjnej dotyczącej cyberzagrożeń. Wynika to z faktu, że organy krajowe nie gromadzą informacji – takich jak informacje udostępniane przez sektor prywatny – i nie dzielą się nimi w sposób systematyczny, co mogłoby pomóc w ocenie stanu cyberbezpieczeństwa w UE. Państwa członkowskie zgłaszają tylko niewielką część incydentów, a wymiana informacji nie jest ani systematyczna, ani kompleksowa²⁴; cyberataki mogą stanowić tylko jeden z aspektów zorganizowanych szkodliwych ataków na europejskie społeczeństwa. Obecnie państwa członkowskie udzielają sobie wzajemnie jedynie ograniczonej pomocy operacyjnej i nie istnieje żaden mechanizm operacyjny umożliwiający współpracę między państwami członkowskimi i instytucjami, agencjami i organami UE w przypadku zaistnienia transgranicznego cyberincydentu lub sytuacji kryzysowej na dużą skalę²⁵.

Poprawa cyberbezpieczeństwa jest zatem niezbędna, aby ludzie ufali innowacjom, łączności i automatyzacji, używali ich i czerpali z nich korzyści, a także aby zapewnić ochronę podstawowych praw i wolności, w tym prawa do prywatności i ochrony danych osobowych oraz wolności wypowiedzi i informacji. Cyberbezpieczeństwo jest niezbędne dla łączności sieciowej oraz globalnego i otwartego internetu, które muszą stanowić podstawę transformacji gospodarki i społeczeństwa w latach 20. XXI wieku. Przyczynia się ono do podnoszenia kwalifikacji i zwiększania zatrudnienia, tworzenia bardziej elastycznych miejsc pracy, bardziej wydajnego i zrównoważonego transportu i rolnictwa oraz łatwiejszego i sprawiedliwszego dostępu do świadczeń zdrowotnych. Ma również zasadnicze znaczenie dla przejścia na czystsza energię w ramach Europejskiego Zielonego Ładu²⁶ dzięki transgranicznym sieciom i inteligentnym licznikom oraz dla uniknięcia niepotrzebnego przechowywania tych samych danych w wielu lokalizacjach. Ponadto ma zasadnicze znaczenie dla międzynarodowego bezpieczeństwa i międzynarodowej stabilności oraz dla

²⁰ <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>

²¹ Oprogramowanie typu ransomware wykorzystano do ataków na szpitale i dokumentację medyczną, np. w Rumunii (czerwiec 2020 r.), w Düsseldorfie (wrzesień 2020 r.) i Vastaamo (październik 2020 r.).

²² PwC, „The Global State of Information Security 2018” [„Stan bezpieczeństwa informacyjnego na świecie 2018”]; ESI Thoughtlab, „The Cybersecurity Imperative” [„Imperatyw cyberbezpieczeństwa”], 2019.

²³ Agencja UE ds. Cyberbezpieczeństwa, „Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA’s Higher Education Skills Database” [„Rozwój umiejętności w dziedzinie cyberbezpieczeństwa w UE: certyfikacja stopni cyberbezpieczeństwa i bazy danych szkolnictwa wyższego ENISA”], grudzień 2019 r.

²⁴ Państwa członkowskie są zobowiązane do przedstawienia grupie współpracy rocznego sprawozdania podsumowującego dotyczącego zgłoszeń otrzymanych na podstawie art. 10 ust. 3 dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa (UE) 2016/1148).

²⁵ Członkowie sieci CSIRT stosują obowiązujące procedury działania dotyczące wzajemnej pomocy.

²⁶ „Europejski Zielony Ład”, COM(2019) 640 final.

rozwoju gospodarek, demokracji i społeczeństw na całym świecie. Rządy, przedsiębiorstwa i osoby prywatne muszą zatem korzystać z narzędzi cyfrowych w sposób odpowiedzialny i ze świadomością kwestii dotyczących bezpieczeństwa. Świadomość i higiena w zakresie cyberbezpieczeństwa muszą stanowić podstawę transformacji cyfrowej codziennej działalności.

Nowa strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę stanowi kluczowy element kształtowania cyfrowej przyszłości Europy²⁷, przygotowanego przez Komisję planu odbudowy dla Europy²⁸, strategii UE w zakresie unii bezpieczeństwa na lata 2020–2025²⁹, globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej³⁰ oraz przygotowanego przez Radę Europejską Programu strategicznego na lata 2019–2024³¹. Określono w niej sposób, w jaki UE będzie chronić swoich obywateli, swoje przedsiębiorstwa i instytucje przed cyberzagrożeniami, rozwijać współpracę międzynarodową oraz pełnić przewodnią rolę w gwarantowaniu globalnego i otwartego internetu.

II. GLOBALNE MYŚLENIE, EUROPEJSKIE DZIAŁANIE

Niniejsza strategia ma na celu zapewnienie globalnego i otwartego internetu, który posiada silne zabezpieczenia umożliwiające sprostanie zagrożeniom dla bezpieczeństwa i podstawowych praw i wolności Europejczyków. Opierając się na postępach osiągniętych w ramach poprzednich strategii, zawiera ona konkretne propozycje dotyczące **stosowania trzech głównych instrumentów – instrumentów regulacyjnych, inwestycyjnych i politycznych** – w celu zajęcia się **trzema obszarami działań UE: 1) odpornością, suwerennością technologiczną i przywództwem, 2) budowaniem zdolności operacyjnych na potrzeby zapobiegania, odstraszenia i reagowania oraz 3) rozwojem globalnej i otwartej cyberprzestrzeni**. UE zamierza wspierać tę strategię za pomocą **realizowanych na bezprecedensową skalę inwestycji w transformację cyfrową UE w ciągu najbliższych siedmiu lat** – potencjalnie czterokrotnie większych niż dotychczas – w ramach nowej polityki technologicznej i przemysłowej oraz programu odbudowy³².

Cyberbezpieczeństwo należy włączyć do wszystkich tych inwestycji cyfrowych, w szczególności dotyczących kluczowych technologii, takich jak sztuczna inteligencja (AI), szyfrowanie i kwantowe technologie obliczeniowe, stosując zachęty, nakładając obowiązki i stosując poziomy odniesienia. Może to pobudzić rozwój europejskiego sektora cyberbezpieczeństwa i dać pewność potrzebną do ułatwienia stopniowego wycofywania dotychczasowych systemów. Europejski Fundusz Obronny (EFO) będzie wspierał europejskie rozwiązania w zakresie cyberobrony w ramach europejskiej bazy technologiczno-przemysłowej sektora obronnego. Cyberbezpieczeństwo uwzględniono

²⁷ Kształtowanie cyfrowej przyszłości Europy, COM(2020) 67 final.

²⁸ Decydujący moment dla Europy: naprawa i przygotowanie na następną generację, COM(2020) 98 final.

²⁹ Strategia UE w zakresie unii bezpieczeństwa na lata 2020–2025, COM(2020) 605 final.

³⁰ https://eeas.europa.eu/topics/eu-global-strategy_en

³¹ <https://www.consilium.europa.eu/pl/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#>

³² Inwestycje w cały łańcuch dostaw technologii cyfrowych, przyczyniające się do transformacji cyfrowej lub do sprostania wynikającym z niej wyzwaniom, powinny stanowić – w formie dotacji i kredytów – co najmniej 20 % – czyli 134,5 mld EUR – z 672,5 mld EUR w ramach Instrumentu na rzecz Odbudowy i Zwiększania Odporności. Finansowanie unijne przewidziane w wieloletnich ramach finansowych na lata 2021–2027 na cyberbezpieczeństwo w ramach programu „Cyfrowa Europa” oraz na badania w dziedzinie cyberbezpieczeństwa w ramach programu „Horyzont Europa”, ze szczególnym uwzględnieniem wsparcia dla MŚP, może wynieść w sumie 2 mld EUR, nie licząc inwestycji ze strony państw członkowskich i przemysłu.

w instrumentach finansowania zewnętrznego służących do wspierania partnerów UE, w szczególności w Instrumencie Sąsiedztwa oraz Współpracy Międzynarodowej i Rozwojowej. Zapobieganie niewłaściwemu wykorzystaniu technologii, ochrona infrastruktury krytycznej oraz zapewnienie integralności łańcuchów dostaw umożliwiają również UE przestrzeganie norm, reguł i zasad ONZ dotyczących odpowiedzialnego zachowania państw³³.

1. ODPORNOŚĆ, SUWERENNOŚĆ TECHNOLOGICZNA I PRZYWÓDZTWO

Unijna infrastruktura krytyczna i usługi podstawowe stają się coraz bardziej współzależne i nabierają coraz bardziej cyfrowego charakteru. Wszystkie urządzenia podłączone do internetu w UE, czy to pojazdy zautomatyzowane, systemy kontroli przemysłowej, czy też urządzenia gospodarstwa domowego, a także całe łańcuchy dostaw, z których te urządzenia pochodzą, muszą być tworzone w sposób uwzględniający bezpieczeństwo na etapie projektowania, być odporne na cyberincydenty i szybko aktualizowane w przypadku wykrycia podatności. Ma to zasadnicze znaczenie dla zapewnienia unijnemu sektorowi prywatnemu i publicznemu możliwości dokonania wyboru spośród najbezpieczniejszych infrastruktur i usług. Najbliższe dziesięciolecie jest dla UE szansą na odegranie wiodącej roli w rozwijaniu bezpiecznych technologii w całym łańcuchu dostaw. W celu zapewnienia odporności i większych możliwości przemysłowych i technologicznych w zakresie cyberbezpieczeństwa należy uruchomić wszystkie niezbędne instrumenty regulacyjne, inwestycyjne i polityczne. Uwzględnianie cyberbezpieczeństwa na etapie projektowania w odniesieniu do procesów, działalności i urządzeń przemysłowych może zmniejszyć ryzyko oraz potencjalnie obniżyć koszty ponoszone przez przedsiębiorstwa i społeczeństwo, a tym samym zwiększyć odporność.

1.1 *Odporna infrastruktura i odporne usługi krytyczne*

Przepisy UE dotyczące bezpieczeństwa sieci i systemów informatycznych stanowią podstawę jednolitego rynku w zakresie cyberbezpieczeństwa. Komisja proponuje reformę tych przepisów w ramach zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji, aby zwiększyć poziom **cyberodporności wszystkich istotnych sektorów, zarówno publicznych, jak i prywatnych, które pełnią ważną funkcję dla gospodarki i społeczeństwa**³⁴. Przegląd jest niezbędny, aby zmniejszyć niespójności na całym rynku wewnętrznym dzięki ujednoliceniu zakresu, wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, krajowego nadzoru i egzekwowania przepisów oraz zdolności właściwych organów.

Znowelizowana dyrektywa w sprawie bezpieczeństwa sieci i informacji będzie stanowiła podstawę bardziej szczegółowych przepisów, które należy również wprowadzić na potrzeby sektorów o strategicznym znaczeniu, w tym energetyki, transportu i zdrowia. Aby zapewnić stosowanie spójnego podejścia zapowiedzianego w strategii w zakresie unii bezpieczeństwa na lata 2020–2025, nowelizacji dyrektywy towarzyszyć będzie przegląd przepisów dotyczących odporności infrastruktury krytycznej³⁵. Technologie energetyczne wykorzystujące elementy cyfrowe oraz bezpieczeństwo powiązanych łańcuchów dostaw są

³³ <https://undocs.org/A/70/174>

³⁴ [wstawić odniesienie do wniosku w sprawie bezpieczeństwa sieci i informacji].

³⁵ [wstawić odniesienie do wniosku dotyczącego dyrektywy w sprawie odporności podmiotów o znaczeniu krytycznym].

istotne dla ciągłości świadczenia podstawowych usług oraz dla strategicznej kontroli nad krytyczną infrastrukturą energetyczną. Komisja zaproponuje zatem odpowiednie środki, w tym „kodeks sieci”, określające zasady cyberbezpieczeństwa w obszarze transgranicznych przepływów energii elektrycznej, które powinny zostać przyjęte do końca 2022 r. Zgodnie z propozycją Komisji również sektor finansowy musi wzmocnić swoją operacyjną odporność cyfrową i zadbać o to, by był w stanie sprostać wszelkiego rodzaju zakłóceniom i zagrożeniom związanym z ICT³⁶. Jeżeli chodzi o transport, Komisja wprowadziła do przepisów UE dotyczących ochrony lotnictwa przepisy dotyczące cyberbezpieczeństwa³⁷ i będzie nadal działać na rzecz zwiększenia cyberodporności we wszystkich rodzajach transportu. Wzmocnienie cyberodporności **procesów i instytucji demokratycznych** stanowi główny element europejskiego planu działania na rzecz demokracji w odniesieniu do ochrony i wspierania wolnych wyborów oraz demokratycznego dyskursu i pluralizmu mediów³⁸. Ponadto z myślą o bezpieczeństwie infrastruktury i usług w ramach przyszłego programu kosmicznego Komisja będzie kontynuować pogłębianie strategii dotyczącej cyberbezpieczeństwa systemu Galileo w odniesieniu do usług w ramach globalnego systemu nawigacji satelitarnej nowej generacji, a także innych nowych elementów programu kosmicznego³⁹.

1.2 Budowa europejskiej tarczy chroniącej przed zagrożeniami dla cyberbezpieczeństwa

Wraz z upowszechnianiem się łączności i coraz większym zaawansowaniem cyberataków istotną funkcję, w tym na poziomie sektorowym, w umożliwianiu wymiany informacji na temat cyberzagrożeń między wieloma zainteresowanymi stronami pełnią ośrodki wymiany i analizy informacji⁴⁰. Poza tym sieci i systemy komputerowe wymagają nieustannego monitorowania i analizy w celu wykrywania włamań i anomalii w czasie rzeczywistym. Wiele prywatnych przedsiębiorstw, organizacji publicznych i organów krajowych utworzyło w związku z tym zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz ośrodki monitorowania bezpieczeństwa.

Ośrodki monitorowania bezpieczeństwa odgrywają kluczową rolę, jeżeli chodzi o gromadzenie plików dzienników⁴¹ oraz wyizolowywanie podejrzanych zdarzeń mających miejsce w ramach sieci łączności, które te ośrodki monitorują. Ich działania opierają się na identyfikacji sygnału i wzorca oraz ekstrakcji wiedzy o zagrożeniach z dużych ilości danych, które wymagają analizy. Przyczyniły się one do wykrywania działań złośliwych plików wykonywalnych i dzięki temu pomogły w powstrzymaniu cyberataków. Biorąc pod uwagę, że praca wykonywana w tych ośrodkach jest bardzo wymagająca i odbywa się pod

³⁶ Wniosek dotyczący rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014, COM(2020) 595 final.

³⁷ Rozporządzenie wykonawcze Komisji 2019/1583.

³⁸ Komunikat w sprawie europejskiego planu działania na rzecz demokracji COM(2020) 790. W ramach planu Europejska Sieć Współpracy w zakresie Wyborów oraz sieci państw członkowskich w zakresie wyborów będą wspierać oddelegowywanie wspólnych zespołów ekspertów w celu zwalczania zagrożeń – w tym zagrożeń dla cyberbezpieczeństwa – dotyczących procesów wyborczych; https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

³⁹ Obejmuje on nową inicjatywę dotyczącą rządowej łączności satelitarnej (Govsatcom) i śmieci kosmicznych (SST).

⁴⁰ <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing>

⁴¹ W taki sposób, aby organy ścigania i organy wymiaru sprawiedliwości mogły je wykorzystać jako dowód.

presją czasu, sztuczna inteligencja oraz w szczególności techniki dotyczące uczenia maszynowego mogą stanowić nieocenione wsparcie dla zatrudnionych w nich osób⁴².

Komisja proponuje utworzenie **sieci ośrodków monitorowania bezpieczeństwa obejmującej całą UE**⁴³, a także wspieranie doskonalenia istniejących ośrodków i tworzenie nowych. Będzie ona także wspierać szkolenie i rozwijanie umiejętności pracowników tych ośrodków. Na podstawie analizy potrzeb przeprowadzonej z udziałem odpowiednich zainteresowanych stron i przy wsparciu Agencji UE ds. Cyberbezpieczeństwa (ENISA) Komisja może przeznaczyć ponad 300 mln EUR na wsparcie współpracy publiczno-prywatnej oraz współpracy transgranicznej przy tworzeniu krajowych i sektorowych sieci, obejmujących także MŚP, w oparciu o odpowiednie zarządzanie, wymianę danych i przepisy dotyczące bezpieczeństwa.

Państwa członkowskie zachęca się do współinwestowania w ten projekt. Dzięki temu ośrodki te będą w stanie prowadzić skuteczniejszą wymianę danych, a także skuteczniej korelować wykryte sygnały i generować wysokiej jakości dane analityczne dotyczące zagrożeń, które będzie można udostępniać ośrodkom wymiany i analizy informacji oraz organom krajowym, co tym samym umożliwi pełniejszą orientację sytuacyjną. Celem będzie połączenie ze sobą – etapowo – możliwie największej liczby ośrodków z całej UE, aby stworzyć zasób zbiorowej wiedzy i dzielić się najlepszymi praktykami. Ośrodki te otrzymają wsparcie, aby mogły szybciej wykrywać i analizować incydenty oraz reagować na nie dzięki możliwościom wynikającym z nowoczesnych technologii z zakresu sztucznej inteligencji i uczenia maszynowego; wsparcie to zostanie uzupełnione infrastrukturą do obliczeń superkomputerowych opracowaną w UE przez Wspólne Przedsięwzięcie w dziedzinie Europejskich Obliczeń Wielkiej Skali⁴⁴.

Dzięki trwałej współpracy za pośrednictwem tej sieci organy i wszystkie zainteresowane strony, w tym wspólna jednostka ds. cyberprzestrzeni (zob. sekcja 2.1), będą otrzymywać wczesne ostrzeżenia dotyczące cyberincydentów. **Sieć ta będzie pełniła funkcję rzeczywistej tarczy chroniącej UE przed zagrożeniami dla cyberbezpieczeństwa**, zapewniając solidną siatkę strażnic, które będą w stanie wykrywać potencjalne zagrożenia, zanim wyrządzą one szkody na dużą skalę.

1.3 Ultrabezpieczna infrastruktura łączności

Rządowa łączność satelitarna Unii Europejskiej⁴⁵, która stanowi element programu kosmicznego, zaoferuje bezpieczne i przystępne cenowo rozwiązania z zakresu łączności w oparciu o przestrzeń kosmiczną, aby umożliwić realizację misji i operacji o krytycznym znaczeniu pod względem ochrony i bezpieczeństwa, którymi zarządzać będą UE i jej państwa

⁴² Źródło: badanie przeprowadzone przez Instytut Badawczy Ponemon, „Improving the Effectiveness of the SOC” [„Zwiększanie skuteczności ośrodków monitorowania bezpieczeństwa”, 2019; aby zapoznać się z badaniami dotyczącymi zastosowania sztucznej inteligencji w ośrodkach monitorowania bezpieczeństwa, zob. na przykład: A. Khraisat, I. Gondal, P. Vamplew i in., „Survey of intrusion detection systems: techniques, datasets and challenges” [„Badanie systemów wykrywania włamań: techniki, zbiory danych i wyzwania”], *Cybersecur* 2, 20, 2019.

⁴³ Wypracowane zostaną bardziej szczegółowe uzgodnienia w zakresie zarządzania, zasad działania oraz finansowania tych ośrodków, a także sposobu, w jaki uzupełnią one istniejące struktury, takie jak ośrodki innowacji cyfrowych.

⁴⁴ <https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking>

⁴⁵ Govsatcom (rządowa łączność satelitarna) stanowi element programu kosmicznego Unii.

członkowskie, w tym podmioty z dziedziny bezpieczeństwa narodowego oraz instytucje, organy i agencje UE.

Państwa członkowskie zobowiązały się do współpracy z Komisją na rzecz wdrożenia na potrzeby Europy bezpiecznej infrastruktury komunikacji kwantowej⁴⁶. W ramach infrastruktury komunikacji kwantowej organy publiczne zyskają zupełnie nowy sposób przekazywania informacji poufnych przy wykorzystaniu ultrabezpiecznej formy szyfrowania stworzonej za pomocą europejskiej technologii, aby chronić się przed cyberatakami. Infrastruktura ta będzie obejmowała dwa główne elementy: istniejące naziemne światłowodowe sieci komunikacyjne łączące strategiczne obszary na poziomie krajowym i transgranicznym; oraz połączone satelity kosmiczne obejmujące całą UE, w tym jej terytoria zamorskie⁴⁷. Inicjatywa ta, której celem jest opracowanie i wdrożenie nowych i bezpieczniejszych form szyfrowania oraz stworzenie nowych sposobów ochrony krytycznych zasobów komunikacyjnych i zasobów danych, może pomóc w zachowaniu bezpieczeństwa informacji szczególnie chronionych i tym samym także infrastruktury krytycznej.

W tej perspektywie, oraz idąc dalej, Komisja zbada możliwość wdrożenia wieloorbitalnego systemu bezpiecznej łączności. W oparciu o Govsatcom i infrastrukturę komunikacji kwantowej system ten łączyłby w sobie nowoczesne technologie (technologię kwantową, sieć 5G, sztuczną inteligencję, przetwarzanie danych na obrzeżach sieci) przy zastosowaniu najbardziej rygorystycznych ram cyberbezpieczeństwa, aby wspierać usługi, w których uwzględniono bezpieczeństwo na etapie projektowania, takie jak niezawodna, bezpieczna i racjonalna pod względem kosztów łączność oraz szyfrowana komunikacja na potrzeby działalności rządowej o krytycznym znaczeniu.

1.4 Zabezpieczenie szerokopasmowych sieci ruchomych nowej generacji

Obywatelom Unii oraz unijnym przedsiębiorstwom korzystającym z zaawansowanych, innowacyjnych aplikacji, które są dostępne dzięki **sieci 5G i sieciom kolejnych generacji**, należy zagwarantować najwyższy standard bezpieczeństwa. Państwa członkowskie wraz z Komisją oraz przy wsparciu ze strony ENISA ustanowiły – przy pomocy unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G⁴⁸ ze stycznia 2020 r. – spójne

⁴⁶ Europejską deklarację w sprawie infrastruktury komunikacji kwantowej podpisała większość państw członkowskich, przy czym rozwój i wdrażanie infrastruktury będą miały miejsce w latach 2021–2027 przy wsparciu finansowym z programów „Horyzont Europa” i „Cyfrowa Europa” oraz Europejskiej Agencji Kosmicznej, pod warunkiem dokonania odpowiednich uzgodnień w zakresie zarządzania; <https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>

⁴⁷ Opracowanie komponentu kosmicznego jest niezbędne, aby osiągnąć długodystansowe połączenia typu punkt-punkt (>1 000 km), których infrastruktura naziemna nie jest w stanie obsłużyć. Wykorzystując właściwości mechaniki kwantowej, infrastruktura komunikacji kwantowej będzie początkowo umożliwiać stronom bezpieczną wymianę losowych tajnych kluczy stosowanych do szyfrowania i odszyfrowywania wiadomości. Opracowanie komponentu kosmicznego będzie obejmowało także wdrożenie infrastruktury na potrzeby testów i zapewnienia zgodności w celu oceny zgodności europejskich urządzeń i systemów do komunikacji kwantowej z infrastrukturą komunikacji kwantowej oraz ich certyfikacji i zatwierdzenia przed włączeniem do infrastruktury komunikacji kwantowej. Komponent ten zostanie opracowany w taki sposób, aby wspierać dodatkowe zastosowania, gdy już osiągną niezbędny poziom dojrzałości technologicznej. Trwający obecnie projekt pilotażowy OpenQKD (<https://openqkd.eu/>) jest prekursorem tej infrastruktury na potrzeby testów i zapewnienia zgodności.

⁴⁸ Komunikat pt. „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi”, COM(2020) 50.

i obiektywne oraz oparte na analizie ryzyka podejście do cyberbezpieczeństwa sieci 5G, które opiera się na ocenie ewentualnych planów ograniczania ryzyka oraz identyfikacji najskuteczniejszych środków. Ponadto UE wzmacnia swoje zdolności w ramach sieci 5G i poza nimi, aby uniknąć zależności i wspierać zrównoważony i zróżnicowany łańcuch dostaw.

W grudniu 2020 r. Komisja opublikowała sprawozdanie na temat skutków zalecenia z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G⁴⁹. Wykazano w nim, że od chwili uzgodnienia zestawu narzędzi poczyniono znaczące postępy oraz że większość państw członkowskich jest na dobrej drodze do zakończenia w najbliższej przyszłości wdrażania znacznej części zestawu narzędzi, choć występują pewne różnice i utrzymujące się luki, które zidentyfikowano już w sprawozdaniu z postępów opublikowanym w lipcu 2020 r.⁵⁰

W październiku 2020 r. Rada Europejska wezwała UE i jej państwa członkowskie do „pełne[go] wykorzystani[a] unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G” oraz do „stosowani[a] odpowiednich ograniczeń wobec dostawców wysokiego ryzyka w odniesieniu do kluczowych aktywów określonych jako krytyczne i wrażliwe w unijnych skoordynowanych ocenach ryzyka” na podstawie wspólnych obiektywnych kryteriów⁵¹.

W przyszłości UE i jej państwa członkowskie powinny zapewnić odpowiednie i skoordynowane ograniczanie wykrytych zagrożeń, w szczególności jeżeli chodzi o cel w postaci ograniczenia do minimum konieczności korzystania z usług dostawców wysokiego ryzyka oraz uniknięcia zależności od tych dostawców na szczeblu krajowym i unijnym, a także uwzględnianie wszelkich nowych znaczących postępów lub zagrożeń. Wzywa się państwa członkowskie do pełnego wykorzystania zestawu narzędzi w ich inwestycjach w zdolności cyfrowe i łączność.

Na podstawie sprawozdania na temat skutków zalecenia z 2019 r. Komisja zachęca państwa członkowskie do przyspieszenia prac z myślą o ukończeniu wdrażania głównych środków przewidzianych w zestawie narzędzi do drugiego kwartału 2021 r. Komisja wzywa także państwa członkowskie do dalszego wspólnego monitorowania poczynionych postępów oraz do zapewniania dalszego ujednolicenia podejść. Aby wspierać ten proces, na szczeblu unijnym będą realizowane trzy główne cele: zapewnianie dalszej konwergencji podejść do łagodzenia ryzyka w całej UE, wspieranie ciągłej wymiany wiedzy i budowania zdolności, a także promowanie odporności łańcucha dostaw i innych strategicznych celów UE w zakresie bezpieczeństwa. Konkretnie działania związane z tymi kluczowymi celami określono w specjalnym dodatku do niniejszego komunikatu.

Komisja będzie kontynuować ścisłą współpracę z państwami członkowskimi, aby zrealizować te cele i działania przy wsparciu ze strony ENISA (zob. dodatek).

Podejście UE oparte na zestawie narzędzi 5G wzbudziło ponadto zainteresowanie państw niebędących członkami UE, które obecnie opracowują własne strategie mające na celu zabezpieczenie ich sieci łączności. Służby Komisji wraz z Europejską Służbą Działań

⁴⁹ Sprawozdanie Komisji na temat skutków zalecenia Komisji z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G, 15 grudnia 2020 r.

⁵⁰ Sprawozdanie grupy współpracy ds. bezpieczeństwa sieci i informacji dotyczące wdrażania zestawu narzędzi na potrzeby cyberbezpieczeństwa, 24 lipca 2020 r.

⁵¹ EUCO 13/20, nadzwyczajne posiedzenie Rady Europejskiej (1 i 2 października 2020 r.) – konkluzje.

Zewnętrznych oraz siecią delegatur Unii są gotowe przekazać organom z całego świata – na ich prośbę – dodatkowe informacje na temat kompleksowego i obiektywnego unijnego podejścia opartego na analizie ryzyka.

1.5 Internet rzeczy zabezpieczonych

Każda połączona z siecią rzecz zawiera podatności, które można wykorzystać, co może nieść za sobą potencjalnie szeroko zakrojone konsekwencje. W zasadach rynku wewnętrznego przewidziano zabezpieczenia przed produktami i usługami, które nie spełniają wymogów bezpieczeństwa. Komisja pracuje już nad zapewnieniem **przejrzystych rozwiązań z zakresu bezpieczeństwa i certyfikacji na podstawie aktu o cyberbezpieczeństwie** oraz nad zachętami do tworzenia bezpiecznych produktów i usług bez uszczerbku dla ich wydajności⁵². W pierwszym kwartale 2021 r. Komisja przyjmie swój pierwszy unijny kroczący program prac (który będzie aktualizowany co najmniej raz na trzy lata), aby umożliwić przemysłowi, organom krajowym i międzynarodowym organom normalizacyjnym przygotowanie się z wyprzedzeniem do przyszłych europejskich programów certyfikacji cyberbezpieczeństwa⁵³. W miarę rozprzestrzeniania się internetu rzeczy konieczne jest zaostreżenie możliwych do wyegzekwowania przepisów, zarówno w celu zapewnienia ogólnej odporności, jak i w celu stymulowania cyberbezpieczeństwa.

Komisja rozważy kompleksowe podejście z uwzględnieniem ewentualnych **nowych horyzontalnych przepisów mających na celu poprawę cyberbezpieczeństwa wszystkich połączonych z siecią produktów i usług towarzyszących wprowadzanych na rynek wewnętrzny**⁵⁴. Takie przepisy mogą obejmować **nowy obowiązek dochowania należytej staranności spoczywający na producentach urządzeń podłączonych do internetu**, zgodnie z którym musieliby oni eliminować luki w oprogramowaniu, w tym stale udostępniać aktualizacje oprogramowania i aktualizacje zabezpieczeń, a także zapewniać – na koniec okresu eksploatacji urządzenia – usunięcie z urządzenia danych osobowych i danych wrażliwych. Przepisy te wzmocniłyby inicjatywę dotyczącą „prawa do naprawy przestarzałego oprogramowania” przedstawioną w planie działania UE dotyczącym gospodarki o obiegu zamkniętym oraz stanowiłyby uzupełnienie bieżących środków odnoszących się do poszczególnych rodzajów produktów, m.in. poprzez wprowadzenie obowiązkowych wymogów, które mają zostać zaproponowane w odniesieniu do dostępu do rynku niektórych urządzeń bezprzewodowych (w drodze aktu delegowanego przyjętego na podstawie dyrektywy w sprawie urządzeń radiowych⁵⁵), a także ustanowienie celu, jakim jest wdrożenie zasad cyberbezpieczeństwa dla pojazdów silnikowych w odniesieniu do

⁵² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). W akcie o cyberbezpieczeństwie propaguje się certyfikację ICT na szczeblu unijnym z europejskimi ramami certyfikacji cyberbezpieczeństwa na potrzeby ustanawiania dobrowolnych europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii, a także w celu ograniczenia fragmentacji rynku wewnętrznego w odniesieniu do programów certyfikacji cyberbezpieczeństwa w Unii. Przedsiębiorstwa „oceniające” cyberbezpieczeństwo mają tym czasem zazwyczaj siedzibę poza UE, a ich przejrzystość i nadzór nad nimi są ograniczone; <https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings>

⁵³ Wymóg określony w art. 47 ust. 5 aktu o cyberbezpieczeństwie.

⁵⁴ W konkluzjach Rady wezwano do wprowadzenia horyzontalnych środków w odniesieniu do cyberbezpieczeństwa urządzeń podłączonych do internetu; 13629/20, 2 grudnia 2020 r.

⁵⁵ Dyrektywa 2014/53/UE.

wszystkich nowych typów pojazdów począwszy od lipca 2022 r.⁵⁶ Ponadto przepisy te opierałyby się na proponowanej rewizji przepisów dotyczących ogólnego bezpieczeństwa produktów, które nie odnoszą się bezpośrednio do aspektów związanych z cyberbezpieczeństwem⁵⁷.

1.6 Większe globalne bezpieczeństwo internetu

Funkcjonalność i integralność internetu na całym świecie zapewnia zestaw kluczowych protokołów; równie ważną rolę w tym względzie pełni infrastruktura pomocnicza⁵⁸. Zestaw ten obejmuje system DNS oraz jego hierarchiczny i delegowany system stref, począwszy od (znajdującej się najwyżej w hierarchii) strefy głównej (root) i 13 głównych serwerów DNS (tzw. serwerów root)⁵⁹, od których zależy funkcjonowanie sieci ogólnoswiatowej (WWW). Komisja zamierza opracować **finansowany ze środków unijnych plan awaryjny umożliwiający reakcję na sytuacje skrajne wpływające na integralność i dostępność globalnego głównego systemu DNS**. Komisja będzie współpracować z ENISA, państwami członkowskimi, dwoma unijnymi operatorami głównego serwera DNS⁶⁰ oraz ze społecznością obejmującą wiele zainteresowanych stron w celu dokonania oceny roli tych operatorów w zapewnianiu globalnej dostępności internetu w każdych okolicznościach.

Aby klient mógł uzyskać dostęp do zasobów udostępnionych pod konkretną nazwą domeny w internecie, jego zapytanie (zazwyczaj o ujednolicony adres zasobów lub URL) musi zostać przetłumaczone – lub „rozwiązane” – na adres IP poprzez odniesienie do serwera nazw DNS. Osoby fizyczne i organizacje w UE coraz bardziej polegają jednak na kilku publicznych resolverach DNS obsługiwanych przez podmioty spoza UE. Taka konsolidacja rozwiązywania nazw DNS w rękach kilku przedsiębiorstw⁶¹ powoduje podatność tego procesu na zagrożenia w przypadku wystąpienia istotnych zdarzeń wpływających na jednego głównego dostawcę oraz sprawia, że organom UE trudniej jest zaradzić możliwym złośliwym cyberatakami oraz poważnym geopolitycznym i technicznym incydentom⁶².

⁵⁶ Zgodnie z regulaminem ONZ przyjętym w czerwcu 2020 r.; <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>

⁵⁷ Rewizja bieżących przepisów dotyczących ogólnego bezpieczeństwa produktów (dyrektywa 2001/95/WE); planuje się również dostosowanie przepisów dotyczących odpowiedzialności producentów w kontekście cyfrowym w zakresie unijnych ram regulacyjnych dotyczących odpowiedzialności.

⁵⁸ „Publiczny rdzeń otwartego internetu, a mianowicie jego główne protokoły i infrastruktura będące dobrem publicznym, zapewniają zasadniczą funkcjonalność internetu jako całości i stanowią podstawę jego normalnego funkcjonowania. ENISA powinna wspierać bezpieczeństwo publicznego rdzenia otwartego internetu i stabilność jego funkcjonowania, w tym m.in. kluczowe protokoły (zwłaszcza DNS, BGP i IPv6), funkcjonowanie systemu nazw domen (jak funkcjonowanie wszystkich domen najwyższego poziomu) i funkcjonowanie strefy rdzennej”; motyw 23 aktu o cyberbezpieczeństwie.

⁵⁹ <https://www.iana.org/domains/root/servers>

⁶⁰ Serwery i.root obsługiwane przez Netnod w Szwecji oraz serwery k.root obsługiwane przez RIPE NCC w Holandii.

⁶¹ „Consolidation in the DNS resolver market – how much, how fast how dangerous?” [„Konsolidacja na rynku resolverów DNS – jej zakres, tempo postępowania i zagrożenia z nią związane”], „Evidence of decreasing Internet entropy – the lack of redundancy in DNS resolution by major websites and services” [„Dowody na zmniejszającą się entropię internetu – brak nadmiarowości przy rozwiązywaniu nazw DNS w przypadku głównych stron internetowych i usług”].

⁶² Istnieją także dowody świadczące o tym, że dane DNS można wykorzystać do celów profilowania, co wpływa na prawo do prywatności i prawo do ochrony danych osobowych.

W celu ograniczenia problemów dotyczących bezpieczeństwa związanych z koncentracją na rynku Komisja zachęci właściwe zainteresowane strony, w tym unijne przedsiębiorstwa, dostawców usług internetowych i dostawców przeglądarek, do przyjęcia strategii dywersyfikacji rozwiązywania nazw DNS. Komisja zamierza także przyczynić się do bezpiecznej łączności internetowej, wspierając rozwój publicznej **europejskiej usługi rozwiązywania nazw DNS**. W ramach inicjatywy „DNS4EU” oferowana będzie alternatywna, europejska usługa dostępu do globalnego internetu. Inicjatywa „DNS4EU” będzie przejrzysta, zgodna z najnowszymi normami i przepisami w zakresie bezpieczeństwa, ochrony danych osobowych oraz uwzględniania ochrony prywatności już w fazie projektowania i domyślnej ochrony prywatności oraz będzie stanowiła element europejskiego sojuszu przemysłowego na rzecz danych i chmury⁶³.

Komisja – we współpracy z państwami członkowskimi i branżą – **zwiększy także tempo absorpcji kluczowych standardów internetowych, w tym IPv6⁶⁴, oraz solidnie ugruntowanych standardów bezpieczeństwa internetu i dobrych praktyk w zakresie DNS, routingu i bezpieczeństwa wiadomości e-mail⁶⁵**, nie wykluczając środków regulacyjnych, takich jak europejska klauzula wygaśnięcia dotycząca protokołu IPv4, w celu ukierunkowania rynku, jeżeli postępy w przyjmowaniu tych standardów będą niewystarczające. UE powinna propagować (na przykład w ramach strategii UE dotyczącej Afryki⁶⁶) wdrażanie tych standardów w krajach partnerskich jako sposób wspierania rozwoju globalnego i otwartego internetu oraz w celu zwalczania zamkniętych i opartych na kontroli modeli internetu. Ponadto Komisja rozważy potrzebę wdrożenia mechanizmu bardziej systematycznego monitorowania i gromadzenia zagregowanych danych na temat ruchu internetowego oraz informowania o potencjalnych zakłóceniach⁶⁷.

1.7 Wzmocniona obecność łańcucha dostaw technologii

UE, przy planowanym wsparciu finansowym na rzecz cyberbezpiecznej transformacji cyfrowej przewidzianym w wieloletnich ramach finansowych na lata 2021–2027, ma niepowtarzalną okazję połączyć swoje zasoby, aby zdynamizować unijną strategię przemysłową⁶⁸ i unijne przywództwo w zakresie technologii cyfrowych i cyberbezpieczeństwa w całym cyfrowym łańcuchu dostaw (z uwzględnieniem danych i chmury, technologii procesorów nowej generacji, ultrabezpiecznej łączności oraz sieci 6G) zgodnie z unijnymi wartościami i priorytetami. Interwencja sektora publicznego powinna opierać się na narzędziach zapewnianych przez unijne ramy regulacyjne w zakresie

⁶³ Joint Declaration: Building the next generation cloud for businesses and the public sector in the EU [Wspólna deklaracja: Budowa chmury nowej generacji dla przedsiębiorstw i sektora publicznego w UE]; <https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe>

⁶⁴ Wdrażanie protokołu IPv6 jest obecnie na bardziej zaawansowanym etapie z uwagi na poważne zmniejszenie podaży i wzrost kosztu adresów IPv4. Jest ono jednak nierównomierne w różnych państwach UE.

⁶⁵ Takie standardy obejmują protokoły DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE oraz normy i dobre praktyki dotyczące routingu, np. wspólnie uzgodnione normy dotyczące bezpieczeństwa routingu (ang. *Mutually Agreed Norms for Routing Security*, MANRS).

⁶⁶ Wspólny komunikat „W kierunku kompleksowej strategii współpracy z Afryką” z dnia 9 marca 2020 r., JOIN(2020) 4 final.

⁶⁷ Takie „obserwatorium internetowe” może wejść w zakres działań Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych; Wniosek dotyczący rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji, COM(2018) 630 final.

⁶⁸ Komunikat pt.: „Nowa strategia przemysłowa dla Europy”, COM(2020) 102 final.

zamówień publicznych oraz ważnych projektach stanowiących przedmiot wspólnego europejskiego zainteresowania. W ramach takiej interwencji można uruchomić inwestycje prywatne poprzez partnerstwa publiczno-prywatne (w tym opierając się na doświadczeniach związanych z partnerstwem publiczno-prywatnym w dziedzinie cyberbezpieczeństwa oraz jego wdrażaniem za pośrednictwem Europejskiej Organizacji ds. Cyberbezpieczeństwa), kapitał wysokiego ryzyka na rzecz MŚP lub sojusze przemysłowe i strategie dotyczące zdolności w zakresie technologii.

Szczególny nacisk zostanie położony także na Instrument Wsparcia Technicznego⁶⁹ oraz najlepsze wykorzystanie przez MŚP najnowszych narzędzi z zakresu cyberbezpieczeństwa – zwłaszcza tych, które nie wchodzą w zakres zmienionej dyrektywy dotyczącej cyberbezpieczeństwa – w tym za pośrednictwem specjalnych działań ośrodków innowacji cyfrowych w ramach programu „Cyfrowa Europa”. Celem jest pozyskanie podobnej kwoty inwestycji ze strony państw członkowskich, uzupełnionej wkładem finansowym w podobnej wysokości wniesionym przez przemysł w ramach partnerstwa zarządzanego wspólnie z państwami członkowskimi w proponowanym **Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji (CCCN)**. CCCN powinny odgrywać kluczową rolę, przy udziale przemysłu i środowisk akademickich, w rozwijaniu suwerenności technologicznej UE w zakresie cyberbezpieczeństwa, budowaniu zdolności do zabezpieczania wrażliwych infrastruktur, takich jak sieć 5G, oraz zmniejszaniu zależności od innych części świata w zakresie najważniejszych technologii.

Komisja zamierza wspierać, potencjalnie za pośrednictwem CCCN, opracowanie specjalnego programu magisterskiego w dziedzinie cyberbezpieczeństwa oraz przyczynić się do opracowania wspólnego europejskiego planu działania na rzecz badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa po 2020 r. Inwestycje za pośrednictwem CCCN opierałyby się również na współpracy w zakresie badań i rozwoju realizowanej przez sieci centrów doskonałości w dziedzinie cyberbezpieczeństwa, zrzeszające najlepsze europejskie zespoły badawcze i przedstawicieli przemysłu z myślą o opracowaniu i wdrożeniu wspólnych programów badawczych, zgodnie z planem działania Europejskiej Organizacji ds. Cyberbezpieczeństwa⁷⁰. Komisja będzie nadal polegać na pracach badawczych prowadzonych przez ENISA i Europol, a także będzie nadal wspierać – w ramach programu „Horyzont Europa” – indywidualnych innowatorów w dziedzinie internetu, którzy opracowują technologie służące ochronie prywatności i bezpiecznej komunikacji na podstawie otwartego oprogramowania i sprzętu komputerowego, jak ma to miejsce obecnie w ramach inicjatywy dotyczącej internetu nowej generacji.

1.8 Siła robocza UE posiadająca umiejętności w dziedzinie cyberbezpieczeństwa

Działania UE na rzecz podnoszenia kwalifikacji siły roboczej, rozwoju, przyciągania i zatrzymywania największych talentów w dziedzinie cyberbezpieczeństwa oraz inwestowania w światowej klasy badania naukowe i innowacje stanowią ważny element ogólnej ochrony przed cyberzagrożeniami. Obszar ten oferuje ogromny potencjał. Szczególną uwagę należy zatem zwrócić na rozwój, przyciąganie i zatrzymywanie bardziej zróżnicowanych talentów. Zmieniony Plan działania w dziedzinie edukacji cyfrowej przyczyni się do podniesienia świadomości w zakresie cyberbezpieczeństwa wśród

⁶⁹ <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0409:FIN>

⁷⁰ <https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies>

obywateli, zwłaszcza dzieci i młodzieży, oraz organizacji, zwłaszcza MŚP⁷¹. Zachęci także do uczestnictwa kobiet w kształceniu w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki („STEM”) oraz do podejmowania pracy w zawodach związanych z ICT poprzez podnoszenie dotychczasowych i nabywanie nowych kwalifikacji w zakresie umiejętności cyfrowych. Ponadto Komisja, wraz z Urzędem Unii Europejskiej ds. Własności Intelektualnej przy Europolu, ENISA, państwami członkowskimi i sektorem prywatnym, opracuje narzędzia służące podnoszeniu świadomości i wytyczne mające na celu zwiększenie odporności przedsiębiorstw UE na **wykorzystujące cyberprzestrzeń kradzieże własności intelektualnej**⁷².

Edukacja – w tym kształcenie i szkolenie zawodowe (VET), świadomość i ćwiczenia – również powinna służyć dalszemu rozwojowi umiejętności w dziedzinie cyberbezpieczeństwa i cyberobrony na szczeblu UE. W tym celu odpowiednie podmioty UE, takie jak ENISA, Europejska Agencja Obrony (EDA), Europejskie Kolegium Bezpieczeństwa i Obrony (EKBiO)⁷³, powinny dążyć do uzyskania synergii między swoimi działaniami.

Inicjatywy strategiczne

UE powinna zapewnić:

- przyjęcie zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji;
- środki regulacyjne dotyczące internetu rzeczy zabezpieczonych;
- inwestycje – za pośrednictwem CCCN – w cyberbezpieczeństwo (w szczególności w ramach programu „Cyfrowa Europa”, „Horyzont Europa” i instrumentu na rzecz odbudowy), które powinny osiągnąć kwotę nawet 4,5 mld EUR w ramach inwestycji publicznych i prywatnych w latach 2021–2027;
- unijną sieć ośrodków monitorowania bezpieczeństwa wspieranych przez sztuczną inteligencję oraz ultrabezpieczną infrastrukturę łączności wykorzystującą technologie kwantowe;
- szerokie zastosowanie technologii cyberbezpieczeństwa poprzez specjalne wsparcie dla MŚP w ramach ośrodków innowacji cyfrowych;
- opracowanie unijnej usługi rozwiązywania nazw DNS jako bezpiecznej i otwartej alternatywy dostępu do internetu dla obywateli, przedsiębiorstw i administracji publicznej w UE; oraz
- zakończenie wdrażania unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G do drugiego kwartału 2021 r. (zob. dodatek).

⁷¹ https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_pl

⁷² https://ec.europa.eu/commission/presscorner/detail/pl/IP_20_2187

⁷³ Za pośrednictwem platformy kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa (ETEE).

2. BUDOWANIE ZDOLNOŚCI OPERACYJNEJ W ZAKRESIE ZAPOBIEGANIA, POWSTRZYMYWANIA I REAGOWANIA

Cyberincydenty, zarówno przypadkowe, jak i celowe działania przestępców, podmiotów państwowych i innych podmiotów niepaństwowych, mogą powodować ogromne szkody. Skala i złożoność tych cyberincydentów, które często wiążą się z wykorzystywaniem usług, sprzętu i oprogramowania osób trzecich, by uzyskać nieuprawniony dostęp do systemu podmiotu lub osoby będących ostatecznym celem ataku, sprawiają, że trudno jest przeciwdziałać kompleksowemu środowisku zagrożeń w UE bez systematycznej i wszechstronnej wymiany informacji i współpracy w zakresie wspólnego reagowania.

Poprzez pełne wdrożenie narzędzi regulacyjnych, mobilizację i współpracę UE dąży do wspierania państw członkowskich w obronie ich obywateli, jak również ich interesów gospodarczych i bezpieczeństwa narodowego, przy pełnym poszanowaniu podstawowych praw i wolności oraz praworządności. Kilka społeczności, na które składają się sieci, instytucje, organy i agencje UE, a także władze państw członkowskich są odpowiedzialne za zapobieganie cyberzagrożeniom, zniechęcanie do nich, powstrzymywanie przed nimi oraz reagowanie na nie przy użyciu swoich odpowiednich instrumentów i inicjatyw⁷⁴. Do społeczności tych należą: (i) organy ds. bezpieczeństwa sieci i informacji, takie jak zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz reagowania na katastrofy; (ii) organy ścigania i organy sądowe; (iii) dyplomacja cyfrowa; oraz (iv) cyberobrona.

2.1 *Wspólna jednostka ds. cyberprzestrzeni*

Wspólna jednostka ds. cyberprzestrzeni służyłaby jako wirtualna i fizyczna platforma współpracy dla-poszczególnych społeczności zajmujących się cyberbezpieczeństwem w UE, z naciskiem na koordynację operacyjną i techniczną w przypadku poważnych transgranicznych cyberincydentów i zagrożeń dla cyberbezpieczeństwa.

Wspólna jednostka ds. cyberprzestrzeni stanowiłaby ważny krok naprzód na drodze do ukończenia tworzenia **unijnych ram reagowania w sytuacji cyberkryzysu**. Jak określono w wytycznych politycznych przewodniczącej Komisji⁷⁵, jednostka ta powinna umożliwić państwom członkowskim oraz instytucjom, organom i agencjom UE pełne wykorzystanie istniejących struktur, zasobów i zdolności oraz propagować podejście oparte na konieczności dzielenia się informacjami („**need to share**”). Zapewniłoby to środki umożliwiające konsolidację dotychczasowych postępów we wdrażaniu zalecenia z 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („plan

⁷⁴ W tym wsparcie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) na rzecz współpracy operacyjnej i zarządzania kryzysowego; sieć CSIRT; sieć organizacji łącznikowej ds. cyberkryzysów (CyCLONe, która zgodnie ze zmienioną dyrektywą w sprawie bezpieczeństwa sieci i informacji ma nosić nazwę EU-CyCLONe); grupa współpracy ds. bezpieczeństwa sieci i informacji; rescEU; Europejskie Centrum ds. Walki z Cyberprzestępczością oraz Wspólna Grupa Zadaniowa ds. Przeciwdziałania Cyberprzestępczości działająca przy Europolu i protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych; Centrum Analiz Wywiadowczych UE (INTCEN) i zestaw narzędzi dla dyplomacji cyfrowej; pojedyncza komórka analiz wywiadowczych (SIAC); projekty cybernetyczne w ramach stałej współpracy strukturalnej (PESCO), w szczególności zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa (CRRT).

⁷⁵ „Unia, która mierzy wyżej. Mój program dla Europy”, Wytyczne polityczne na następną kadencję Komisji Europejskiej (2019–2024) kandydatki na przewodniczącą Komisji Europejskiej Ursuli von der Leyen.

działania”)⁷⁶. Stworzyłoby to również możliwość dalszego zacieśniania współpracy w zakresie struktury planu działania i wykorzystania osiągniętych postępów, zwłaszcza w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji oraz sieci CyCLONe.

W ten sposób można by wyeliminować **dwie główne luki**, które obecnie zwiększają podatność na transgraniczne zagrożenia i incydenty mające wpływ na Unię i skutkują nieefektywnym reagowaniem na nie. Po pierwsze, **społeczności** cywilne, dyplomatyczne, organów ścigania oraz obronne zajmujące się cyberbezpieczeństwem nie mają jeszcze wspólnej przestrzeni, w której mogłyby rozwijać zorganizowaną współpracę i która ułatwiałaby współpracę operacyjną i techniczną. Po drugie, odpowiednie zainteresowane strony w dziedzinie cyberbezpieczeństwa nie były jak dotąd w stanie w pełni wykorzystać **potencjału** współpracy operacyjnej i wzajemnej pomocy w ramach istniejących sieci i społeczności. W tym kontekście należy również wskazać na brak platformy umożliwiającej współpracę operacyjną z sektorem prywatnym. Wspomniana jednostka powinna poprawić i przyspieszyć koordynację oraz umożliwić UE stawienie czoła cyberincydentom i cyberkryzysom na dużą skalę oraz reagowanie na nie.

Wspólna jednostka ds. cyberprzestrzeni nie byłaby dodatkowym, samodzielnym organem ani nie ograniczałaby kompetencji i uprawnień krajowych organów ds. cyberbezpieczeństwa lub uczestników z UE. Jednostka ta działałaby raczej na zasadzie mechanizmu ochronnego, w ramach którego uczestnicy mogliby korzystać ze wzajemnego wsparcia i wiedzy fachowej, zwłaszcza wówczas, gdy różne cyberspołeczności byłyby zmuszone do ścisłej współpracy. Jednocześnie ostatnie wydarzenia wskazują na konieczność zwiększenia przez UE poziomu ambicji i gotowości do zmierzenia się z krajobrazem i realiami cyberzagrożeń. W ramach wkładu w utworzenie wspólnej jednostki ds. cyberprzestrzeni podmioty unijne (Komisja oraz agencje i organy UE) będą zatem gotowe istotnie zwiększyć swoje zasoby i zdolności, tak by znacznie poprawić swoją gotowość i odporność.

Wspólna jednostka ds. cyberprzestrzeni spełniałaby trzy główne cele. Po pierwsze, zapewniłaby **gotowość** wszystkich społeczności zajmujących się cyberbezpieczeństwem; po drugie, zapewniłaby stałą, wspólną **orientację** sytuacyjną poprzez dzielenie się informacjami; po trzecie, wzmocniłaby skoordynowaną **reakcję** na incydenty i skoordynowane działania mające na celu przywrócenie funkcjonowania zaatakowanych systemów. Aby osiągnąć te cele, jednostka powinna opierać się na dobrze zdefiniowanych **modułach i celach**, takich jak zagwarantowanie **bezpiecznej i szybkiej wymiany informacji**, poprawa **współpracy** między uczestnikami, w tym interakcji między państwami członkowskimi i odpowiednimi podmiotami UE, ustanowienie zorganizowanych **partnerstw z zaufaną bazą przemysłową** oraz ułatwienie skoordynowanego podejścia do **współpracy z partnerami zewnętrznymi**. W tym celu jednostka mogłaby ułatwić opracowanie ram współpracy w oparciu o inwentaryzację dostępnych zdolności na szczeblu krajowym i unijnym.

Aby wspólna jednostka ds. cyberprzestrzeni stała się centralnym elementem współpracy operacyjnej UE w zakresie cyberbezpieczeństwa, Komisja będzie współpracować z państwami członkowskimi oraz odpowiednimi instytucjami, organami i agencjami UE, w tym ENISA, CERT-UE i Europolem, w celu promowania **stopniowego i integracyjnego podejścia**, przy pełnym poszanowaniu kompetencji i mandatów wszystkich zaangażowanych stron. Zgodnie z tym podejściem wspomniana jednostka mogłaby przyczynić się do

⁷⁶ Zalecenie dotyczące planu działania C(2017) 6100 final z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

zacieśniania współpracy między podmiotami z konkretnej cyberspołeczności, jeżeli podmioty te uznają to za konieczne.

Proponuje się, by proces tworzenia wspólnej jednostki ds. cyberprzestrzeni przebiegał w czterech głównych etapach:

- *zdefiniowanie* – poprzez inwentaryzację dostępnych zdolności na szczeblu krajowym i unijnym;
- *przygotowanie* – poprzez ustanowienie ram dla zorganizowanej współpracy i pomocy;
- *wprowadzenie* – poprzez wdrożenie ram wykorzystujących zasoby zapewnione przez uczestników, tak aby wspólna jednostka ds. cyberprzestrzeni zyskała zdolność operacyjną;
- *rozszerzenie* – poprzez wzmocnienie zdolności skoordynowanego reagowania z udziałem przemysłu i partnerów.

Wykorzystując wyniki konsultacji z państwami członkowskimi, instytucjami, organami i agencjami UE⁷⁷, do lutego 2021 r. Komisja, z udziałem Wysokiego Przedstawiciela – zgodnie z jego kompetencjami – przedstawi proces, główne etapy i harmonogram działań mających na celu **zdefiniowanie, przygotowanie, wprowadzenie i rozszerzenie wspólnej jednostki ds. cyberprzestrzeni**.

2.2 Zwalczanie cyberprzestępczości

Nasza zależność od narzędzi internetowych gwałtownie zwiększyła powierzchnię ataku dla cyberprzestępców i doprowadziła do sytuacji, w której dochodzenia w sprawie niemal wszystkich rodzajów przestępstw mają element cyfrowy. Ponadto fundamentom naszego społeczeństwa zagrażają podmioty działające w cyberprzestrzeni oraz te, które wykorzystują cybernarzędzia do planowania i realizacji nielegalnych działań. Istnieją zatem ścisłe powiązania z ogólną polityką bezpieczeństwa UE, odzwierciedlone w związanych z cyberprzestrzenią aspektach strategii UE w zakresie unii bezpieczeństwa z 2020 r. oraz w agendzie antyterrorystycznej dla UE⁷⁸.

Kluczowym czynnikiem w zapewnieniu cyberbezpieczeństwa jest zwalczanie cyberprzestępczości: aby osiągnąć skuteczny efekt odstraszający, nie wystarczy sama odporność – konieczne jest również identyfikowanie i ściganie przestępców. Dlatego tak ważne jest rozwijanie współpracy i wymiany między podmiotami odpowiedzialnymi za cyberbezpieczeństwo i organami ścigania. W związku z tym na szczeblu unijnym Europol i ENISA wypracowały już mechanizmy skutecznej współpracy w zakresie organizacji wspólnych konferencji i warsztatów, a także opracowywania wspólnych sprawozdań dla Komisji, państw członkowskich i innych zainteresowanych stron na temat zagrożeń dla cyberbezpieczeństwa i wyzwań technologicznych. Komisja będzie w dalszym ciągu wspierać

⁷⁷ Konsultacje z państwami członkowskimi (w tym podczas spotkania szefów krajowych organów ds. cyberbezpieczeństwa Blue OLEx20), instytucjami, organami i agencjami UE przeprowadzone w okresie od lipca do listopada 2020 r.

⁷⁸ Komunikat „Plan dla UE w dziedzinie walki z terroryzmem: przewidywanie, zapobieganie, ochrona i reagowanie”, 9.12.2020 r., COM(2020) 795 final.

to zintegrowane podejście mające na celu zapewnienie spójnego i skutecznego reagowania w oparciu o wyczerpujące informacje.

Jednym z ważnych elementów tego reagowania jest konieczność, aby organy unijne i krajowe zwiększyły i poprawiły zdolność organów ścigania do prowadzenia dochodzeń dotyczących cyberprzestępczości przy pełnym poszanowaniu praw podstawowych i dążeniu do zapewnienia wymaganej równowagi między różnymi prawami i interesami. UE powinna być w stanie zwalczać cyberprzestępczość za pomocą w pełni wdrożonego i odpowiedniego prawodawstwa, ze szczególnym naciskiem na zwalczanie niegodziwego traktowania dzieci w celach seksualnych w internecie oraz na dochodzenia w cyberprzestrzeni, w tym w celu zwalczania przestępczości w ciemnej sieci. Organy ścigania muszą być w pełni przygotowane do prowadzenia dochodzeń w cyberprzestrzeni. W związku z tym Komisja przedstawi plan działania w zakresie poprawy zdolności cyfrowych organów ścigania poprzez zapewnienie im niezbędnych umiejętności i narzędzi. Ponadto Europol będzie nadal rozwijał swoją rolę jako centrum wiedzy fachowej, aby wspierać krajowe organy ścigania w zwalczaniu przestępczości wykorzystującej cyberprzestrzeń oraz cyberprzestępstw, przyczyniając się do określenia wspólnych standardów kryminalistycznych (za pośrednictwem laboratorium i centrum innowacji Europolu). Wszystkie te działania wymagają odpowiedniego wdrożenia przez państwa członkowskie, które zachęca się do korzystania z krajowych programów finansowanych z Funduszu Bezpieczeństwa Wewnętrznego oraz do proponowania projektów w odpowiedzi na zaproszenia do składania wniosków w ramach instrumentu tematycznego.

Komisja wykorzysta wszystkie odpowiednie środki, w tym postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego, aby zapewnić pełną transpozycję i wdrożenie dyrektywy z 2013 r. dotyczącej ataków na systemy informatyczne⁷⁹, w tym realizację przez państwa członkowskie obowiązku przekazywania statystyk. Będzie skuteczniej zapobiegać nadużywaniu nazw domen, w tym, w stosownych przypadkach, rozpowszechnianiu nielegalnych treści, oraz dążyć do zapewnienia dostępności dokładnych danych rejestracyjnych poprzez dalszą współpracę z Internetową Korporacją ds. Nadanych Nazw i Numerów (ICANN) i innymi zainteresowanymi stronami w ramach systemu zarządzania internetem, w szczególności za pośrednictwem grupy roboczej ds. bezpieczeństwa publicznego przy Rządowym Komitecie Doradczym ICANN. W związku z tym we wniosku dotyczącym zmienionej dyrektywy w sprawie bezpieczeństwa sieci i informacji przewidziano prowadzenie dokładnych i kompletnych baz danych zawierających nazwy domen i dane rejestracyjne, czyli „dane WHOIS”, oraz zapewnienie zgodnego z prawem dostępu do takich danych, co jest niezbędne do zagwarantowania bezpieczeństwa, stabilności i odporności systemu nazw domen.

Komisja będzie również kontynuować prace nad zapewnieniem odpowiednich kanałów dostępu i wyjaśnieniem zasad uzyskiwania transgranicznego dostępu do elektronicznego materiału dowodowego na potrzeby dochodzeń w sprawach karnych (potrzebnego w 85 % dochodzeń, przy czym 65 % wszystkich wniosków kierowanych jest do usługodawców mających siedzibę w innej jurysdykcji), poprzez ułatwienie przyjęcia, a następnie wdrożenia „pakietu w sprawie elektronicznego materiału dowodowego” i środków praktycznych⁸⁰.

⁷⁹ Dyrektywa 2013/40/UE dotycząca ataków na systemy informatyczne.

⁸⁰ COM(2018) 225 i 226; C(2020) 2779 final. W szczególności projekt SIRIUS otrzymał niedawno dodatkowe środki finansowe w ramach Instrumentu Partnerstwa na poprawę kanałów umożliwiających uzyskanie zgodnego z prawem transgranicznego dostępu do elektronicznego materiału dowodowego na potrzeby dochodzeń

Ważne jest szybkie przyjęcie przez Parlament Europejski i Radę wniosków w sprawie elektronicznego materiału dowodowego, aby udostępnić to skuteczne narzędzie funkcjonariuszom. Elektroniczny materiał dowodowy musi być możliwy do odczytania, dlatego też Komisja będzie nadal pracować nad wspieraniem zdolności organów ścigania w dziedzinie dochodzeń w cyberprzestrzeni, w tym nad rozwiązaniem problemu zaszyfrowanych treści napotykanym w toku dochodzeń w sprawach karnych, przy jednoczesnym pełnym zachowaniu funkcji szyfrowania, jaką jest ochrona praw podstawowych i cyberbezpieczeństwa.

2.3 *Unijny zestaw narzędzi dla dyplomacji cyfrowej*

UE stosuje **zestaw narzędzi dla dyplomacji cyfrowej**⁸¹ w celu zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania przed nimi i reagowania na nie. Po wprowadzeniu w maju 2019 r. ram prawnych dotyczących ukierunkowanych środków ograniczających przeciwko cyberatakom⁸² w lipcu 2020 r. UE umieściła w wykazie sześć osób i trzy podmioty odpowiedzialne za cyberataki wobec UE i jej państw członkowskich lub zaangażowane w takie ataki⁸³. W październiku 2020 r. umieszczono w wykazie kolejne dwie osoby i jeden podmiot⁸⁴. Szkodliwe działania w cyberprzestrzeni, w tym działania z opóźnionym skutkiem, należy zwalczać poprzez skuteczną i kompleksową wspólną unijną reakcję dyplomatyczną, z wykorzystaniem pełnego zakresu środków dostępnych na szczeblu UE.

Szybka i skuteczna wspólna unijna reakcja dyplomatyczna wymaga solidnej wspólnej orientacji sytuacyjnej oraz zdolności do szybkiego przygotowania wspólnego stanowiska UE. Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa będzie zachęcał do ustanowienia **unijnej grupy roboczej ds. cyberwywiadu państw członkowskich** działającej przy Centrum Analiz Wywiadowczych UE (INTCEN) oraz ułatwiał jej ustanowienie, z myślą o rozwijaniu strategicznej współpracy wywiadowczej w zakresie cyberzagrożeń i działań w cyberprzestrzeni. Prace te przyczynią się do dalszego wspierania orientacji sytuacyjnej UE i podejmowania decyzji dotyczących wspólnej reakcji

w sprawach karnych (potrzebne w 85 % dochodzeń w sprawie poważnych przestępstw, przy czym 65 % wszystkich wniosków kierowanych jest do usługodawców mających siedzibę w innej jurysdykcji), a także na ustanowienie równoważnych przepisów na szczeblu międzynarodowym.

⁸¹ <https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>

⁸² Decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129I z 17.5.2019, s. 13); oraz rozporządzenie Rady (UE) 2019/796

z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129I z 17.5.2019, s. 1).

⁸³ Decyzja Rady (WPZiB) 2020/1127 z dnia 30 lipca 2020 r. zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (ST/9564/2020/INIT) (Dz.U. L 246 z 30.7.2020, s. 12); rozporządzenie wykonawcze Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (ST/9568/2020/INIT) (Dz.U. L 246 z 30.7.2020, s. 4).

⁸⁴ Decyzja Rady (WPZiB) 2020/1537 z dnia 22 października 2020 r. zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 351I z 22.10.2020, s. 5); rozporządzenie wykonawcze Rady (UE) 2020/1536 z dnia 22 października 2020 r. wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 351I z 22.10.2020, s. 1).

dyplomatycznej. Grupa robocza ma współpracować z istniejącymi strukturami⁸⁵, w tym w razie potrzeby ze strukturami, które zajmują się szerszymi zagrożeniami związanymi z hybrydową i obcą ingerencją, w celu gromadzenia informacji pozwalających uzyskać orientację sytuacyjną i w celu oceny tej orientacji.

Aby wzmocnić swoją zdolność do zapobiegania szkodliwym zachowaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania przed nimi oraz reagowania na nie, Wysoki Przedstawiciel – z udziałem Komisji zgodnie z jej kompetencjami – przedstawi wniosek przewidujący określenie przez UE swojej **postawy w zakresie cyberprewencji**. Postawa ta, uwzględniająca dotychczasowe prace w ramach zestawu narzędzi dla dyplomacji cyfrowej, powinna przyczynić się do odpowiedzialnego zachowania państw i współpracy w cyberprzestrzeni oraz nadać określony kierunek walce z tymi cyberatakami, które mają najbardziej znaczące skutki, zwłaszcza tymi, które mają wpływ na naszą infrastrukturę krytyczną, nasze instytucje i procesy demokratyczne⁸⁶, a także atakami w ramach łańcucha dostaw oraz wykorzystującą cyberprzestrzeń kradzieżą własności intelektualnej. W ramach wspomnianej postawy należy określić, w jaki sposób UE i państwa członkowskie mogłyby wykorzystać swoje polityczne, gospodarcze, dyplomatyczne, prawne i strategiczne narzędzia komunikacji przeciwko szkodliwym działaniom w cyberprzestrzeni, a także określić, w jaki sposób UE i państwa członkowskie mogłyby zwiększyć swoją zdolność do atrybucji szkodliwych działań w cyberprzestrzeni. Ponadto Wysoki Przedstawiciel – w porozumieniu z Radą oraz Komisją – zamierza przeanalizować **dodatkowe środki w ramach zestawu narzędzi dla dyplomacji cyfrowej**, w tym możliwość wprowadzenia dalszych wariantów środków ograniczających, a także rozważyć możliwość **głosowania większością kwalifikowaną w przypadku wpisów do wykazu w ramach horyzontalnego systemu sankcji za cyberataki**. Co więcej, UE powinna podjąć dalsze działania na rzecz **zacieśnienia współpracy z partnerami międzynarodowymi**, w tym z NATO, w celu poszerzenia wspólnego zrozumienia krajobrazu zagrożeń, opracowania mechanizmów współpracy i określenia wspólnych reakcji dyplomatycznych.

Wysoki Przedstawiciel – z udziałem Komisji – zaproponuje również aktualizację **wytycznych dotyczących wdrażania zestawu narzędzi dla dyplomacji cyfrowej**⁸⁷, w tym z myślą o zwiększeniu skuteczności procesu decyzyjnego, oraz będzie nadal regularnie organizować ćwiczenia, jak również oceny dotyczące zestawu narzędzi dla dyplomacji cyfrowej. Ponadto UE powinna w dalszym ciągu **włączać zestaw narzędzi dla dyplomacji cyfrowej do unijnych mechanizmów kryzysowych**, dążyć do osiągnięcia synergii z działaniami na rzecz przeciwdziałania zagrożeniom hybrydowym, dezinformacji i obcej ingerencji w ramach wspólnych ram dotyczących zwalczania zagrożeń hybrydowych⁸⁸ i europejskiego planu działania na rzecz demokracji. W tym kontekście UE powinna przeanalizować interakcję między zestawem narzędzi dla dyplomacji cyfrowej a ewentualnym zastosowaniem art. 42 ust. 7 TUE i art. 222 TFUE⁸⁹.

⁸⁵ Takimi jak pojedyncza komórka analiz wywiadowczych UE (SIAC) oraz, w razie potrzeby, odpowiednimi projektami ustanowionymi w ramach PESCO, a także systemem wczesnego ostrzegania z 2018 r., który utworzono w celu wspierania ogólnego podejścia UE do rozwiązywania problemu dezinformacji.

⁸⁶ W szczególności poprzez dążenie do osiągnięcia synergii z inicjatywami w ramach europejskiego planu działania na rzecz demokracji.

⁸⁷ 13007/17.

⁸⁸ <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>

⁸⁹ Odpowiednio klauzuli wzajemnej obrony i klauzuli solidarności.

2.4 Wzmocnienie zdolności w zakresie cyberobrony

UE i państwa członkowskie muszą zwiększyć swoją zdolność do zapobiegania cyberzagrożeniom i reagowania na nie zgodnie z unijnym poziomem ambicji wynikającym z globalnej strategii UE z 2016 r.⁹⁰ W tym celu Wysoki Przedstawiciel, we współpracy z Komisją, przedstawi **przegląd ram polityki w zakresie cyberobrony**, aby wzmocnić dalszą koordynację i współpracę między podmiotami UE⁹¹, jak również z państwami członkowskimi i między nimi, w tym w odniesieniu do misji i operacji w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO). Ramy polityki w zakresie cyberobrony powinny stanowić podstawę przyszłego strategicznego kompasu⁹², zapewniając dalsze włączanie kwestii cyberbezpieczeństwa i cyberobrony do szerszego programu działań w zakresie bezpieczeństwa i obrony.

W 2018 r. UE uznała cyberprzestrzeń za sferę operacyjną⁹³. Przyszła „**wojskowa wizja i strategia dotycząca cyberprzestrzeni jako sfery operacyjnej**” opracowywana przez Komitet Wojskowy UE powinna doprecyzować, w jaki sposób cyberprzestrzeń jako sfera operacyjna umożliwia prowadzenie misji i operacji wojskowych UE w dziedzinie WPBiO. Utworzona przez Europejską Agencję Obrony (EDA) **wojskowa sieć CERT**⁹⁴ przyczyni się do dalszego znacznego zacieśnienia współpracy między państwami członkowskimi. Ponadto w celu zapewnienia cyberbezpieczeństwa krytycznej infrastruktury kosmicznej wchodzącej w zakres kompetencji programu kosmicznego Agencja Unii Europejskiej ds. Programu Kosmicznego, a w szczególności centrum monitorowania bezpieczeństwa systemu Galileo, zostanie wzmocniona, a jej mandat rozszerzony na inne krytyczne zasoby programu kosmicznego.

UE i państwa członkowskie powinny zapewnić dalszy bodziec do **rozwijania najnowocześniejszych zdolności w zakresie cyberobrony** za pomocą różnych polityk i instrumentów UE, zwłaszcza ram polityki UE w zakresie cyberobrony, a w stosownych przypadkach w oparciu o prace EDA. Wymaga to położenia silnego nacisku na rozwijanie i wykorzystywanie kluczowych technologii, takich jak AI, szyfrowanie i kwantowe technologie obliczeniowe. Zgodnie z priorytetami UE w zakresie rozwoju zdolności z 2018 r.⁹⁵ oraz w oparciu o ustalenia zawarte w pierwszym pełnym sprawozdaniu dotyczącym skoordynowanego rocznego przeglądu w zakresie obronności (CARD)⁹⁶ UE powinna w dalszym ciągu wspierać współpracę między państwami członkowskimi w zakresie **badania, innowacji i rozwoju zdolności w dziedzinie cyberobrony**, zachęcając

⁹⁰ Konkluzje Rady (14149/16) w sprawie realizacji globalnej strategii UE w dziedzinie bezpieczeństwa i obrony.

⁹¹ W szczególności ESDZ, w tym Sztabem Wojskowym Unii Europejskiej (EUMS), Europejskim Kolegium Bezpieczeństwa i Obrony (EKBiO), Komisją oraz agencjami UE, zwłaszcza Europejską Agencją Obrony (EDA).

⁹² Konkluzje Rady w sprawie bezpieczeństwa i obrony z dnia 17 czerwca 2020 r. (8910/20).

⁹³ <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pl/pdf>

⁹⁴ Utworzenie unijnej wojskowej sieci CERT odpowiada celowi określonymu w ramach polityki UE w zakresie cyberobrony w 2018 r. i ma na celu promowanie aktywnej interakcji i wymiany informacji między wojskowymi CERT państw członkowskich UE.

⁹⁵ W czerwcu 2018 r. państwa członkowskie uzgodniły w ramach Rady Sterującej EDA, że będą kierować współpracą w dziedzinie obrony na szczeblu UE.

⁹⁶ Zatwierdzonym przez ministrów obrony w Radzie Sterującej EDA w listopadzie 2020 r.

[https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-\(card\)](https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card))

państwa członkowskie do pełnego wykorzystania potencjału **stalej współpracy strukturalnej (PESCO)**⁹⁷ oraz **EFO**⁹⁸.

Przyszły **plan działania Komisji na rzecz synergii między przemysłem cywilnym, obronnym i kosmicznym**, który ma zostać przedstawiony w pierwszym kwartale 2021 r., będzie obejmował działania mające na celu dalsze wspieranie synergii na poziomie programów, technologii, innowacji i przedsiębiorstw typu *start-up*, zgodnie z zasadami zarządzania odpowiednimi programami⁹⁹.

Ponadto należy stworzyć odpowiednie synergie i interfejsy między inicjatywami w zakresie cyberobrony podejmowanymi w kontekście innych ram, w tym opartymi na współpracy projektami związanymi z cyberprzestrzenią¹⁰⁰ realizowanymi przez państwa członkowskie w ramach PESCO, a także ze strukturami cyberbezpieczeństwa UE, w celu wspierania wymiany informacji i wzajemnego wsparcia.

Inicjatywy strategiczne

UE powinna:

- ukończyć prace nad unijnymi ramami reagowania w sytuacji cyberkryzysu i określić proces, etapy i harmonogram budowy wspólnej jednostki ds. cyberprzestrzeni;
- kontynuować wdrażanie programu dotyczącego cyberprzestępczości w ramach strategii w zakresie unii bezpieczeństwa;
- wspierać i ułatwiać tworzenie grupy roboczej państw członkowskich ds. cyberwywiadu przy INTCEN UE;
- wzmocnić pozycję UE w zakresie cyberprewencji w celu zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania przed nimi i reagowania na nie;
- dokonać przeglądu ram polityki w zakresie cyberobrony;
- ułatwiać opracowanie unijnej „wojskowej wizji i strategii dotyczącej cyberprzestrzeni jako sfery operacyjnej” na potrzeby misji i operacji wojskowych w dziedzinie WPBiO;
- wspierać synergie między przemysłem cywilnym, obronnym i kosmicznym; oraz
- wzmocnić cyberbezpieczeństwo krytycznej infrastruktury kosmicznej w ramach programu kosmicznego.

⁹⁷ Obecnie istnieje kilka projektów PESCO związanych z cyberprzestrzenią, w szczególności Platforma wymiany informacji o cyberzagrożeniach i reagowaniu na cyberincydenty, Zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa, Cyberakademia i centrum innowacji UE oraz Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji (CIDCC).

⁹⁸ W ramach EFO Komisja zidentyfikowała już możliwe obszary wspólnych działań w zakresie badań i rozwoju w dziedzinie cyberobrony, których celem jest wzmocnienie współpracy, zdolności innowacyjnych i konkurencyjności przemysłu obronnego.

⁹⁹ Takimi jak „Horyzont Europa”, „Cyfrowa Europa” i EFO.

¹⁰⁰ <https://pesco.europa.eu/>

3. ROZWIJANIE GLOBALNEJ I OTWARTEJ CYBERPRZESTRZENI

UE powinna nadal współpracować z partnerami międzynarodowymi w celu promowania politycznego modelu i wizji cyberprzestrzeni opartych na praworządności, prawach człowieka, podstawowych wolnościach i wartościach demokratycznych, które przyczyniają się do rozwoju społecznego, gospodarczego i politycznego na całym świecie oraz do tworzenia unii bezpieczeństwa. Współpraca międzynarodowa ma zasadnicze znaczenie dla utrzymania globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni. W tym celu UE powinna kontynuować współpracę z państwami trzecimi, organizacjami międzynarodowymi oraz społecznością obejmującą wiele zainteresowanych stron, aby opracować i wdrożyć spójną i całościową międzynarodową politykę w dziedzinie cyberbezpieczeństwa, mając na uwadze rosnące wzajemne połączenia między gospodarczymi aspektami nowych technologii, bezpieczeństwem wewnętrznym oraz polityką zagraniczną, bezpieczeństwa i obrony. UE, jako silny blok gospodarczy i handlowy oparty na podstawowych wartościach demokratycznych, poszanowaniu praworządności i praw podstawowych, ma również wyjątkową pozycję, aby odgrywać wiodącą rolę w procesie formułowania i promowania międzynarodowych norm i standardów.

3.1 Wiodąca rola UE w zakresie standardów, norm i ram w cyberprzestrzeni

Wzmocnienie międzynarodowej normalizacji

W celu promowania i obrony swojej wizji cyberprzestrzeni na szczeblu międzynarodowym UE musi **zwiększyć swoje zaangażowanie w międzynarodowe procesy normalizacji i wzmocnić swoją wiodącą rolę w tych procesach oraz zwiększyć swoją reprezentację w międzynarodowych i europejskich organach normalizacyjnych, jak również w innych organizacjach opracowujących normy**¹⁰¹. Ponieważ technologie cyfrowe rozwijają się w szybkim tempie, normy międzynarodowe mają coraz większe znaczenie jako uzupełnienie tradycyjnych działań regulacyjnych w dziedzinach takich jak AI, chmura, kwantowe technologie obliczeniowe i komunikacja kwantowa. Państwa trzecie coraz częściej wykorzystują międzynarodową normalizację w celu realizacji swoich programów politycznych i ideologicznych, co często nie jest zgodne z wartościami UE. Ponadto istnieje coraz większe ryzyko istnienia konkurujących ram międzynarodowej normalizacji, co prowadzi do fragmentacji.

Kształtowanie norm międzynarodowych w dziedzinie nowych technologii i podstawowej architektury internetu zgodnie z wartościami UE ma zasadnicze znaczenie dla zapewnienia, aby internet pozostał globalny i otwarty, technologie były ukierunkowane na człowieka i skoncentrowane na prywatności, a korzystanie z nich – zgodne z prawem, bezpieczne i etyczne. W ramach przyszłej strategii normalizacyjnej UE powinna określić swoje **cele w zakresie międzynarodowej normalizacji** oraz prowadzić aktywne i skoordynowane działania informacyjne mające promować je na szczeblu międzynarodowym. Należy dążyć do ściślejszej współpracy i podziału obciążenia z mającymi podobne poglądy partnerami i europejskimi zainteresowanymi stronami.

¹⁰¹ Np. [Międzynarodowa Organizacja Normalizacyjna \(ISO\)](#), [Międzynarodowa Komisja Elektrotechniczna \(IEC\)](#), [Międzynarodowy Związek Telekomunikacyjny \(ITU\)](#), [Europejski Komitet Normalizacyjny \(CEN\)](#), [Europejski Komitet Normalizacyjny Elektrotechniki \(CENELEC\)](#), [Europejski Instytut Norm Telekomunikacyjnych \(ETSI\)](#), grupa zadaniowa Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) oraz [Instytut Inżynierów Elektryków i Elektroników \(IEEE\)](#).

Promocja odpowiedzialnego zachowania państw w cyberprzestrzeni

UE kontynuuje współpracę z partnerami międzynarodowymi na rzecz rozwoju i promowania globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni, w której przestrzega się **prawa międzynarodowego, w szczególności Karty Narodów Zjednoczonych**¹⁰², oraz **postępuje się zgodnie z dobrowolnymi, niewiążącymi normami, przepisami i zasadami odpowiedzialnego zachowania państwa**¹⁰³. Wraz z osłabieniem skutecznej wielostronnej debaty na temat międzynarodowego bezpieczeństwa w cyberprzestrzeni istnieje wyraźna potrzeba zajęcia przez UE i państwa członkowskie bardziej aktywnego stanowiska w dyskusjach na forum ONZ i innych odpowiednich forach międzynarodowych. UE jest najbardziej kompetentna, aby **rozwijać, koordynować i konsolidować stanowiska państw członkowskich na forach międzynarodowych i powinna przygotować stanowisko UE w sprawie stosowania prawa międzynarodowego w cyberprzestrzeni**. Wysoki Przedstawiciel, wraz z państwami członkowskimi, zamierza również przedstawić integracyjną i opartą na konsensusie propozycję zobowiązania politycznego w sprawie **programu działania na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni**¹⁰⁴ w ramach ONZ. Plan działania – który opiera się na istniejącym dorobku prawnym UE zatwierdzonym przez Zgromadzenie Ogólne ONZ¹⁰⁵ – miałby stanowić platformę współpracy i wymiany najlepszych praktyk w ramach ONZ i zawiera propozycję ustanowienia mechanizmu umożliwiającego wprowadzenie w życie norm odpowiedzialnego zachowania państw i promowanie budowania zdolności. Ponadto celem Wysokiego Przedstawiciela jest skuteczniejsze wdrażanie i zachęcanie do wdrażania **środków budowy zaufania** między państwami, w tym poprzez wymianę najlepszych praktyk na poziomie regionalnym i wielostronnym oraz przyczynianie się do współpracy międzyregionalnej.

Rozwój globalnej infrastruktury komunikacyjnej nie powinien prowadzić do cenzury, masowej inwigilacji, naruszania ochrony danych oraz represji wobec społeczeństwa obywatelskiego, środowiska akademickiego i obywateli. UE powinna nadal odgrywać wiodącą rolę w zakresie ochrony i promowania **praw człowieka i podstawowych wolności** w internecie. W tym celu UE powinna promować dalsze przestrzeganie międzynarodowych przepisów i norm dotyczących praw człowieka¹⁰⁶ oraz wdrożyć plan działania dotyczący praw człowieka i demokracji na lata 2020–2024¹⁰⁷, a także opracować Wytoczne UE w sprawie praw człowieka dotyczące wolności wypowiedzi w internecie i poza nim¹⁰⁸, **nadając nowy impuls praktycznemu stosowaniu instrumentów UE**. UE powinna podejmować nieustanne starania na rzecz **ochrony obrońców praw człowieka, społeczeństwa obywatelskiego i przedstawicieli środowiska akademickiego zajmujących się takimi kwestiami, jak cyberbezpieczeństwo, ochrona danych osobowych, niejawni**

¹⁰² <https://www.un.org/en/sections/un-charter/un-charter-full-text/>

¹⁰³ O których mowa w odpowiednich sprawozdaniach grupy ekspertów rządowych ds. ewolucji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego, zatwierdzonych przez Zgromadzenie Ogólne ONZ, w szczególności za lata 2015, 2013 i 2010.

¹⁰⁴ <https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf>

¹⁰⁵ Jak wynika z odpowiednich sprawozdań grupy ekspertów rządowych ds. ewolucji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego, zatwierdzonych przez Zgromadzenie Ogólne ONZ, w szczególności za lata 2015, 2013 i 2010.

¹⁰⁶ W szczególności Karty Narodów Zjednoczonych i Powszechnej deklaracji praw człowieka.

¹⁰⁷ <https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/>

¹⁰⁸ <https://www.consilium.europa.eu/media/28348/142549.pdf>

nadzór i cenzura online. W tym celu UE powinna zapewnić dalsze praktyczne wytyczne, promować najlepsze praktyki i zwiększyć starania na rzecz zapobiegania niewłaściwemu wykorzystaniu powstających technologii, zwłaszcza poprzez stosowanie w stosownych przypadkach środków dyplomatycznych, a także kontrolę wywozu takich technologii. UE powinna również w dalszym ciągu walczyć o ochronę członków społeczeństwa najbardziej narażonych na zagrożenia w internecie, proponując przepisy mające na celu lepszą ochronę dzieci przed wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych oraz strategię na rzecz praw dziecka.

Budapeszteńska Konwencja o cyberprzestępczości

UE nie przestaje wspierać państw trzecich, które chcą przystąpić do **budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości**, oraz nieprzerwanie prowadzi prace nad sfinalizowaniem **drugiego Protokołu dodatkowego do budapeszteńskiej Konwencji o cyberprzestępczości**, który przewiduje środki i gwarancje mające na celu poprawę współpracy międzynarodowej między organami ścigania i organami sądowymi, a także między organami i usługodawcami w innych państwach, i w przypadku którego Komisja uczestniczy w negocjacjach w imieniu UE¹⁰⁹. Obecna inicjatywa na rzecz nowego instrumentu prawnego dotyczącego cyberprzestępczości na szczepku ONZ grozi pogłębieniem podziałów i spowolnieniem bardzo potrzebnych reform krajowych oraz związanych z nimi działań na rzecz budowania zdolności, co może utrudnić skuteczną współpracę międzynarodową przy zwalczaniu cyberprzestępczości: UE nie widzi potrzeby wprowadzania na szczepku ONZ żadnego nowego instrumentu prawnego dotyczącego cyberprzestępczości. UE w dalszym ciągu angażuje się w **wielostronną wymianę informacji na temat cyberprzestępczości**, aby zapewnić poszanowanie praw człowieka i podstawowych wolności poprzez inkluzywność, przejrzystość i uwzględnienie dostępnej wiedzy fachowej, z myślą o zapewnieniu wartości dodanej dla wszystkich.

3.2 Współpraca z partnerami i społecznością obejmującą wiele zainteresowanych stron

UE powinna **pogłębiać i rozszerzać dialog w sprawach cyberprzestrzeni z państwami trzecimi**, aby promować swoje wartości i wizję cyberprzestrzeni, wymieniać się najlepszymi praktykami i dążyć do skuteczniejszej współpracy. UE powinna również rozpocząć **zorganizowaną wymianę z organizacjami regionalnymi**, takimi jak Unia Afrykańska, Forum Regionalne ASEAN, Organizacja Państw Amerykańskich oraz Organizacja Bezpieczeństwa i Współpracy w Europie. Jednocześnie UE powinna starać się znaleźć, w miarę możliwości, wspólną płaszczyznę porozumienia z innymi partnerami w oparciu o kwestie będące przedmiotem wspólnego zainteresowania. We współpracy z delegaturami Unii, a także w stosownych przypadkach z ambasadami państw członkowskich na całym świecie, UE powinna utworzyć nieformalną **unijną sieć dyplomacji cyfrowej** służącą promowaniu unijnej wizji cyberprzestrzeni, wymianie informacji i regularnej koordynacji działań w zakresie cyberprzestrzeni¹¹⁰.

W oparciu o wspólne deklaracje z dnia 8 lipca 2016 r.¹¹¹ i z dnia 10 lipca 2018 r.¹¹² UE powinna nadal rozwijać **współpracę UE–NATO**, w szczególności w zakresie wymogów

¹⁰⁹ Decyzja Rady z czerwca 2019 r. (nr ref. 9116/19).

¹¹⁰ W stosownych przypadkach mogłaby ona również wykorzystywać działania nieformalnej sieci dyplomacji cyfrowej UE zrzeszającej ministerstwa spraw zagranicznych państw członkowskich.

¹¹¹ <http://www.consilium.europa.eu/pl/press/press-releases/2016/07/08-eu-nato-joint-declaration/>

¹¹² <https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/>

dotyczących interoperacyjności w dziedzinie cyberobrony. W tym kontekście UE powinna w dalszym ciągu dążyć do włączenia odpowiednich struktur WPBiO do sfederalizowanej sieci misyjnej NATO, umożliwiając w razie potrzeby interoperacyjność sieci z NATO i partnerami. Ponadto należy przeanalizować dalsze możliwości współpracy między UE a NATO w zakresie edukacji, szkolenia i ćwiczeń, w tym poprzez poszukiwanie synergii między Europejskim Kolegium Bezpieczeństwa i Obrony a działającym pod auspicjami NATO Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Cyberatakami.

Zgodnie ze swoimi wartościami UE zdecydowanie wspiera i promuje **model zarządzania internetem zakładający udział w tym procesie wielu zainteresowanych stron**. Żaden pojedynczy podmiot, rząd ani żadna organizacja międzynarodowa nie powinny dążyć do kontrolowania internetu. UE powinna nadal angażować się w prace for¹¹³, których celem jest zacieśnianie współpracy i zapewnianie ochrony podstawowych praw i wolności, zwłaszcza prawa do godności, prywatności oraz wolności wypowiedzi i informacji. Aby rozwijać wielostronną współpracę w zakresie cyberbezpieczeństwa, Komisja i Wysoki Przedstawiciel – zgodnie ze swoimi odpowiednimi kompetencjami – dążą do wzmocnienia **regularnych i zorganizowanych kontaktów z zainteresowanymi stronami**, w tym z sektorem prywatnym, środowiskiem akademickim i społeczeństwem obywatelskim, podkreślając, że liczne wzajemne powiązania, jakie charakteryzują cyberprzestrzeń, powodują dla wszystkich zainteresowanych stron konieczność wymieniania się informacjami oraz przyjęcia konkretnych obowiązków w celu utrzymania globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni. Starania te będą stanowić cenny wkład w potencjalne kluczowe działania na szczęblu UE.

3.3 Wzmacnianie globalnych zdolności w celu zwiększenia globalnej odporności

Aby zapewnić wszystkim krajom możliwość czerpania społecznych, gospodarczych i politycznych korzyści z internetu i korzystania z technologii, UE stale wspiera swoich partnerów w zwiększaniu ich cyberodporności i zdolności do prowadzenia dochodzeń w sprawie cyberprzestępczości i jej ścigania oraz przeciwdziałania cyberzagrożeniom. Aby zapewnić ogólną spójność, UE powinna opracować **program na rzecz budowania zewnętrznych zdolności cyfrowych UE** w celu kierowania tymi działaniami zgodnie z wytycznymi dotyczącymi budowania przez UE zewnętrznych zdolności cyfrowych¹¹⁴ oraz Agendą na rzecz zrównoważonego rozwoju 2030¹¹⁵. W programie należy wykorzystać wiedzę fachową państw członkowskich i odpowiednich instytucji, organów i agencji UE oraz wiedzę fachową zdobywaną w ramach inicjatyw, w tym unijnej sieci na rzecz budowania zdolności cyfrowych¹¹⁶, zgodnie z ich odpowiednimi mandatami. Należy powołać **unijną Radę ds. Budowania Zdolności Cyfrowych**, która zrzeszałaby odpowiednie zainteresowane strony instytucjonalne z UE oraz monitorowała postępy, a także identyfikowała dalsze synergie i potencjalne luki. Mogłaby ona ponadto wspierać wzmocnioną współpracę z państwami członkowskimi, jak również z partnerami z sektora publicznego i prywatnego oraz innymi odpowiednimi organami międzynarodowymi, aby zapewnić koordynację działań i uniknąć ich powielania.

¹¹³ Takie jak Internetowa Korporacja ds. Nadanych Nazw i Numerów (ICANN) i Forum Zarządzania Internetem (IGF).

¹¹⁴ <https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf>

¹¹⁵ https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm

¹¹⁶ <https://www.eucybernet.eu/>

W procesie **budowy zdolności cyfrowych UE** należy nadal koncentrować się na Bałkanach Zachodnich i krajach sąsiadujących z UE, a także na krajach partnerskich doświadczających szybkiego rozwoju cyfrowego. Działania UE powinny wspierać rozwój ustawodawstwa i polityki krajów partnerskich zgodnie z odpowiednimi politykami i standardami unijnej dyplomacji cyfrowej. W tym kontekście starania UE na rzecz budowania zdolności w dziedzinie transformacji cyfrowej powinny obejmować standardowo cyberbezpieczeństwo. W tym celu UE powinna opracować program szkoleniowy skierowany do pracowników UE odpowiedzialnych za realizację działań w zakresie budowania przez UE zewnętrznych zdolności cyfrowych i cybernetycznych. UE powinna również pomagać tym krajom w mierzeniu się z coraz większym wyzwaniem, jakim są szkodliwe działania w cyberprzestrzeni, które szkodzą rozwojowi ich społeczeństw oraz **integralności i bezpieczeństwu systemów demokratycznych**, zgodnie ze staraniami podejmowanymi w ramach europejskiego planu działania na rzecz demokracji. W tym względzie szczególnie przydatne mogłoby być uczenie się poprzez wymianę informacji i wiedzy między państwami członkowskimi UE, jak również odpowiednimi agencjami UE i państwami trzecimi.

Ponadto, w kontekście umowy w zakresie cywilnego wymiaru WPBiO z 2018 r.¹¹⁷, cywilne misje w dziedzinie WPBiO mogą również przyczynić się do szerszej reakcji UE na wyzwania związane z cyberbezpieczeństwem, w szczególności poprzez wzmocnienie praworządności w krajach partnerskich, jak również zdolności organów ścigania i administracji cywilnej.

Inicjatywy strategiczne

UE powinna:

- określić zbiór celów w procesach normalizacji międzynarodowej i promować je na szczeblu międzynarodowym;
- promować międzynarodowe bezpieczeństwo i stabilność w cyberprzestrzeni, w szczególności poprzez przedstawienie przez UE i jej państwa członkowskie projektu programu działania na rzecz promocji odpowiedzialnego zachowania państw w cyberprzestrzeni w ramach Organizacji Narodów Zjednoczonych;
- oferować praktyczne wytyczne dotyczące stosowania praw człowieka i podstawowych wolności w cyberprzestrzeni;
- lepiej chronić dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, a także opracować strategię na rzecz praw dziecka;
- wzmocnić i promować budapeszteńską Konwencję o cyberprzestępczości, w tym poprzez prace nad drugim Protokołem dodatkowym do tej konwencji;
- zintensyfikować unijny dialog w sprawach cyberprzestrzeni z państwami trzecimi, organizacjami regionalnymi i międzynarodowymi, w tym poprzez nieformalną unijną sieć dyplomacji cyfrowej;
- wzmocnić kontakty ze społecznością skupiającą wiele zainteresowanych stron, zwłaszcza poprzez regularną i zorganizowaną wymianę z sektorem prywatnym,

¹¹⁷ <https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/pl/pdf>

środowiskiem akademickim i społeczeństwem obywatelskim; oraz

- zaproponować program na rzecz budowania zewnętrznych zdolności cyfrowych UE oraz powołać unijną Radę ds. Budowania Zdolności Cyfrowych.

III. CYBERBEZPIECZEŃSTWO W INSTYTUCJACH, ORGANACH I AGENCJACH UE

Instytucje, organy i agencje UE – ze względu na ich wysoką rangę polityczną, ważne zadania polegające na koordynacji bardzo delikatnych kwestii oraz rolę w zarządzaniu dużymi kwotami ze środków publicznych – **są regularnym celem cyberataków**, a zwłaszcza cyberszpiegostwa. Poszczególne instytucje, organy i agencje UE różnią się jednak znacznie, jeśli chodzi o poziom ich cyberodporności i zdolności do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie oraz związaną z tym dojrzałość. Konieczne jest zatem zwiększenie ogólnego poziomu cyberbezpieczeństwa poprzez przyjęcie spójnych i jednolitych zasad.

W dziedzinie bezpieczeństwa informacji poczyniono postępy w kierunku większej spójności **przepisów dotyczących ochrony informacji niejawnych UE, jak również szczególnie chronionych informacji jawnych**. Interoperacyjność systemów informacji niejawnych pozostaje jednak ograniczona, co uniemożliwia bezproblemowe przekazywanie informacji między poszczególnymi podmiotami. Konieczne są dalsze postępy w celu wypracowania międzyinstytucjonalnego podejścia do przetwarzania informacji niejawnych UE i szczególnie chronionych informacji jawnych, które mogłoby również służyć jako wzór interoperacyjności w państwach członkowskich. Należy również ustanowić poziom odniesienia służący uproszczeniu procedur w kontaktach z państwami członkowskimi. UE powinna też dalej rozwijać swoją zdolność komunikowania się w bezpieczny sposób z odpowiednimi partnerami, w możliwie największym stopniu opierając się na istniejących rozwiązaniach i procedurach.

W związku z tym, zgodnie z zapowiedzią zawartą w strategii w zakresie unii bezpieczeństwa, Komisja przedstawi **w 2021 r. wnioski dotyczące wspólnych wiążących zasad bezpieczeństwa informacji oraz wspólnych wiążących zasad cyberbezpieczeństwa dla wszystkich instytucji, organów i agencji UE**, w oparciu o trwające obecnie między instytucjami UE rozmowy poświęcone cyberbezpieczeństwu¹¹⁸.

Obecne i przyszłe tendencje w zakresie telepracy będą również wymagały dalszych inwestycji w bezpieczny sprzęt, infrastrukturę i narzędzia pozwalające na pracę zdalną na dokumentach poufnych i niejawnych.

Ponadto coraz bardziej nieprzyjazny krajobraz cyberzagrożeń i większa częstotliwość występowania bardziej wyrafinowanych cyberataków dotyczących instytucje, organy i agencje UE sprawiają, że w celu osiągnięcia wysokiego poziomu dojrzałości cybernetycznej konieczne są większe inwestycje. Powstaje program mający na celu zwiększenie świadomości pracowników wszystkich instytucji, organów i agencji UE w zakresie cyberbezpieczeństwa, higieny cyberbezpieczeństwa i wspierania wspólnej kultury cyberbezpieczeństwa.

¹¹⁸ Regularne rozmowy między instytucjami UE na temat cyberbezpieczeństwa stanowią część szerszej wymiany poglądów na temat możliwości i wyzwań związanych z transformacją cyfrową, którym muszą sprostać instytucje UE.

Aby zwiększyć zdolność CERT-UE do pomagania instytucjom, organom i agencjom UE w stosowaniu nowych zasad cyberbezpieczeństwa i poprawić ich cyberodporność, konieczne jest **wzmocnienie tego zespołu poprzez wprowadzenie skuteczniejszego mechanizmu finansowania**. Należy również wzmocnić mandat CERT-UE, aby zapewnić mu stabilne środki na realizację tych celów.

Inicjatywy strategiczne

1. Rozporządzenie w sprawie bezpieczeństwa informacji w instytucjach, organach i agencjach UE
2. Rozporządzenie w sprawie wspólnych zasad cyberbezpieczeństwa dla instytucji, organów i agencji UE
3. Nowa podstawa prawna dla CERT-UE w celu wzmocnienia jego mandatu i finansowania

IV. WNIOSKI

Spójne wdrożenie niniejszej strategii przyczyni się do zapewnienia UE cyberbezpiecznej cyfrowej dekady, realizacji unii bezpieczeństwa oraz wzmocnienia pozycji UE na świecie.

UE powinna odgrywać wiodącą rolę w opracowywaniu standardów i norm na potrzeby światowej klasy rozwiązań oraz norm z zakresu cyberbezpieczeństwa na potrzeby podstawowych usług i infrastruktury krytycznej, jak również w rozwijaniu i stosowaniu nowych technologii. Każda organizacja i każda osoba korzystająca z internetu jest częścią rozwiązania zapewniającego cyberbezpieczną transformację cyfrową.

Komisja i Wysoki Przedstawiciel – zgodnie ze swoimi odpowiednimi kompetencjami – będą monitorować postępy w realizacji założeń niniejszej strategii i opracują kryteria oceny. Wkład w ten proces monitorowania powinny stanowić m.in. sprawozdania ENISA oraz regularne sprawozdania Komisji dotyczące unii bezpieczeństwa. Wyniki przyczynią się do realizacji celów przyszłej cyfrowej dekady¹¹⁹. Zgodnie ze swoimi odpowiednimi kompetencjami Komisja i Wysoki Przedstawiciel będą nadal współpracować z państwami członkowskimi w celu określenia praktycznych środków, które w razie potrzeby pozwolą połączyć siły czterech społeczności zajmujących się w UE cyberbezpieczeństwem, a działających w obszarach: infrastruktury krytycznej i odporności rynku wewnętrznego, wymiaru sprawiedliwości i egzekwowania prawa, dyplomacji cyfrowej oraz cyberobrony. Ponadto Komisja i Wysoki Przedstawiciel będą nadal współpracować ze społecznością obejmującą wiele zainteresowanych stron, podkreślając konieczność odegrania przez każdą osobę korzystającą z internetu swojej roli w utrzymaniu globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni, w której każdy może bezpiecznie prowadzić życie cyfrowe.

¹¹⁹ Zgodnie z zapowiedzią w programie prac Komisji na 2021 r.

Dodatek: Kolejne kroki w zakresie cyberbezpieczeństwa sieci 5G

W oparciu o wyniki przeglądu zalecenia Komisji w sprawie cyberbezpieczeństwa sieci 5G¹²⁰ w kolejnych etapach skoordynowanych prac na szczeblu UE należy skoncentrować się na trzech kluczowych celach oraz na głównych działaniach krótko- i średnioterminowych przedstawionych w poniższej tabeli, które mają zostać wdrożone przez organy państw członkowskich, Komisję i ENISA.

Pierwszą kwestią priorytetową na kolejnym etapie jest **zakończenie wdrażania zestawu narzędzi na szczeblu krajowym oraz zajęcie się kwestiami wskazanymi w sprawozdaniu z postępów z lipca 2020 r.** W tym kontekście niektóre strategiczne środki z zestawu narzędzi skorzystałyby na **usprawnionej koordynacji prac lub wymianie informacji** w ramach specjalnej grupy roboczej ds. bezpieczeństwa sieci i systemów informatycznych, jak już wskazano w sprawozdaniu z postępów, co mogłoby potencjalnie doprowadzić do opracowania **najlepszych praktyk lub wytycznych**. Jeśli chodzi o środki techniczne, ENISA mogłaby zapewnić dalsze wsparcie, opierając się na pracy, którą już wykonała, i bardziej szczegółowo analizując niektóre zagadnienia, a także **opracowując kompleksowy przegląd wszystkich istotnych wytycznych dotyczących wymogów w zakresie cyberbezpieczeństwa sieci 5G dla operatorów sieci ruchomej**.

Po drugie, w celu umożliwienia **identyfikowania nowych lub pojawiających się zagrożeń i reagowania na nie** państwa członkowskie podkreśliły znaczenie nadążania za zmianami dzięki **stałemu monitorowaniu postępów technologicznych, architektury sieci 5G, zagrożeń oraz przypadków użycia i zastosowań sieci 5G, a także czynników zewnętrznych**. Ponadto we wstępnej analizie ryzyka należy dokładniej przyjrzeć się szeregowi aspektów, w szczególności w celu zapewnienia, aby obejmowała ona cały ekosystem 5G, w tym wszystkie istotne elementy infrastruktury sieci i łańcucha dostaw 5G. Chociaż zestaw narzędzi opracowano jako elastyczny instrument, który można dostosowywać, aby zapewnić jego kompleksowość i aktualność, w stosownych przypadkach w perspektywie średnioterminowej można by podjąć kroki mające na celu jego rozszerzenie lub zmianę.

Po trzecie, należy nadal podejmować **działania na szczeblu UE** mające wspierać i uzupełniać cele zestawu narzędzi oraz włączać je w pełni do odpowiednich polityk Unii i Komisji, w szczególności realizując działania zapowiedziane przez Komisję w komunikacie w sprawie zestawu narzędzi z dnia 29 stycznia 2020 r.¹²¹ w wielu obszarach (np. unijne finansowanie bezpiecznych sieci 5G, inwestycje w technologie 5G i technologie będące następcą 5G, instrumenty ochrony handlu i konkurencji w celu uniknięcia zakłóceń na rynku dostaw 5G itp.).

W stosownych przypadkach na początku 2021 r. najważniejsze podmioty powinny dokonać szczegółowych ustaleń i uzgodnić cele pośrednie w odniesieniu do głównych działań określonych poniżej.

¹²⁰ Sprawozdanie Komisji na temat skutków zalecenia Komisji 2019/534 z dnia 26 marca 2019 r. w sprawie cyberbezpieczeństwa sieci 5G.

¹²¹ Komunikat Komisji COM(2020) 50 pt. „Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi”, 29 stycznia 2020 r.

Główny cel 1: Zapewnienie spójnych podejść krajowych w celu skutecznego ograniczania ryzyka w całej UE		
Obszary	Główne działania krótko- i średnioterminowe	Najważniejsze podmioty
Wdrożenie zestawu narzędzi przez państwa członkowskie	Zakończenie wdrażania środków zalecanych we wnioskach dotyczących zestawu narzędzi do drugiego kwartału 2021 r. wraz z okresową inwentaryzacją w ramach grupy roboczej ds. bezpieczeństwa sieci i systemów informatycznych.	Organy państw członkowskich
Wymiana informacji i najlepszych praktyk w zakresie środków strategicznych związanych z dostawcami	Intensywniejsza wymiana informacji i rozważenie możliwych najlepszych praktyk, w szczególności w zakresie: <ul style="list-style-type: none"> - ograniczeń dotyczących dostawców wysokiego ryzyka (SM03) oraz środków związanych ze świadczeniem usług zarządzanych (SM04); - bezpieczeństwa i odporności łańcucha dostaw, w szczególności w następstwie badania przeprowadzonego przez BEREC na temat SM05–SM06. 	Organy państw członkowskich, Komisja
Budowanie zdolności i wytyczne dotyczące środków technicznych	Prowadzenie szczegółowych analiz technicznych oraz opracowanie wspólnych wytycznych i narzędzi, w tym: <ul style="list-style-type: none"> - kompleksowej i dynamicznej matrycy środków kontroli bezpieczeństwa i najlepszych praktyk w zakresie bezpieczeństwa sieci 5G; wytycznych wspierających wdrażanie wybranych środków technicznych z zestawu narzędzi.	ENISA, organy państw członkowskich
Główny cel 2: Wspieranie ciągłej wymiany wiedzy i budowania zdolności		
Obszary	Główne działania krótko- i średnioterminowe	Najważniejsze podmioty
Ciągłe gromadzenie wiedzy	Organizowanie działań w zakresie gromadzenia wiedzy na temat technologii i związanych z nią wyzwań (architektury otwarte, cechy sieci 5G – np. wirtualizacja, konteneryzacja, warstwowanie itp.), zmian krajobrazu zagrożeń, rzeczywistych incydentów itp.	ENISA, organy państw członkowskich, inne zainteresowane strony
Oceny ryzyka	Aktualizacja i wymiana informacji na temat zaktualizowanych krajowych ocen ryzyka	Organy państw członkowskich, Komisja, ENISA
Wspólne projekty finansowane przez UE wspierające wdrażanie zestawu narzędzi	Zapewnienie wsparcia finansowego dla projektów wspierających wdrażanie zestawu narzędzi z wykorzystaniem finansowania unijnego, w szczególności w ramach programu „Cyfrowa Europa” (np. projektów służących budowaniu zdolności organów krajowych, stanowisk badawczych lub innych zaawansowanych zdolności itp.)	Organy państw członkowskich, Komisja
Współpraca zainteresowanych stron	Wspieranie współpracy i współdziałania między organami krajowymi zajmującymi się cyberbezpieczeństwem sieci 5G (np. grupą współpracy ds. bezpieczeństwa sieci i informacji, organami ds. cyberbezpieczeństwa, organami regulacyjnymi ds. telekomunikacji) oraz z podmiotami prywatnymi.	Organy państw członkowskich, Komisja, ENISA

Główny cel 3: Promowanie odporności łańcucha dostaw i innych strategicznych celów UE w zakresie bezpieczeństwa		
Obszary	Główne działania krótko- i średnioterminowe	Najważniejsze podmioty
Normalizacja	Określenie i wdrożenie konkretnego planu działania na rzecz zwiększenia reprezentacji UE w organach normalizacyjnych w ramach kolejnych etapów prac podgrupy ds. bezpieczeństwa sieci i informacji w zakresie normalizacji, aby zrealizować konkretne cele w zakresie bezpieczeństwa, w tym promowanie interoperacyjnych interfejsów, aby ułatwić dywersyfikację dostawców.	Organy państw członkowskich
Odporność łańcucha dostaw	<ul style="list-style-type: none"> – Przeprowadzenie szczegółowej analizy ekosystemu i łańcucha dostaw 5G w celu poprawy identyfikowania i monitorowania kluczowych zasobów i potencjalnych krytycznych zależności – Zapewnienie, aby rynek i łańcuch dostaw 5G funkcjonowały zgodnie z regułami i celami UE w zakresie handlu i konkurencji określonymi w komunikacie Komisji z dnia 29 stycznia oraz aby inwestycje, których realizacja potencjalnie wpływa na łańcuch wartości 5G, były objęte mechanizmem monitorowania BIZ, z uwzględnieniem celów, jakie przyświecają zestawowi narzędzi – Monitorowanie istniejących i oczekiwanych tendencji rynkowych oraz ocena ryzyka i możliwości w dziedzinie otwartej sieci dostępu radiowego, w szczególności za pomocą niezależnego badania 	Organy państw członkowskich, Komisja
Certyfikacja	Rozpoczęcie przygotowania odpowiednich propozycji systemów certyfikacji dla kluczowych komponentów sieci 5G i funkcjonujących u dostawców procesów, aby pomóc w przeciwdziałaniu określonym zagrożeniom związanym z podatnościami o charakterze technicznym określonymi w planach ograniczania ryzyka w ramach zestawu narzędzi.	Komisja, ENISA, organy krajowe, inne zainteresowane strony
Zdolności UE i bezpieczne wdrażanie sieci	<ul style="list-style-type: none"> – Inwestowanie w badania naukowe i innowacje oraz w zdolności, w szczególności poprzez przyjęcie partnerstwa na rzecz inteligentnych sieci i usług – Wdrożenie odpowiednich warunków w zakresie bezpieczeństwa na potrzeby unijnych programów finansowania i instrumentów finansowych (wewnętrznych i zewnętrznych) zgodnie z zapowiedzią zawartą w komunikacie Komisji z dnia 29 stycznia. 	Państwa członkowskie, Komisja, zainteresowane strony z sektora sieci 5G
Aspekty zewnętrzne	Pozytywne rozpatrywanie wniosków państw trzecich, które chciałyby zrozumieć opracowane przez UE podejście oparte na zestawie narzędzi i potencjalnie z niego korzystać.	Państwa członkowskie, Komisja ESDZ, delegatury Unii