II

(Akty o charakterze nieustawodawczym)

ZALECENIA

ZALECENIE KOMISJI (UE) 2021/1086

z dnia 23 czerwca 2021 r.

w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Cyberbezpieczeństwo ma zasadnicze znaczenie dla powodzenia transformacji cyfrowej gospodarki i społeczeństwa. UE zobowiązała się do bezprecedensowego poziomu inwestycji, aby zapewnić zaufanie obywateli, przedsiębiorstw i organów publicznych do narzędzi cyfrowych.

(2) Pandemia COVID-19 zwiększyła znaczenie łączności i stabilności sieci i systemów informatycznych, od których uzależniona jest Europa, a także wykazała potrzebę ochrony całego łańcucha dostaw. Niezawodne i bezpieczne sieci i systemy informatyczne mają szczególne znaczenie dla podmiotów na pierwszej linii walki z pandemią, takich jak szpitale, agencje medyczne i producenci szczepionek. Koordynacja wysiłków UE na rzecz zapobiegania cyberatakom o najpoważniejszych skutkach wymierzonym przeciwko takim podmiotom, wykrywania ich, zniechęcania do nich, powstrzymywania ich, łagodzenia ich skutków i reagowania na nie mogłaby zapobiec przypadkom utraty życia i próbom osłabienia zdolności UE do jak najszybszego pokonania pandemii. Ponadto wzmocnienie zdolności UE do skutecznego przeciwdziałania cyberatakom przyczynia się do rozwoju globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni.

(3) W obliczu transgranicznego charakteru zagrożeń dla cyberbezpieczeństwa oraz ciągłego narastania coraz bardziej złożonych, wszechobecnych i ukierunkowanych ataków ([1]) odpowiednie instytucje i podmioty działające w dziedzinie cyberbezpieczeństwa powinny zwiększyć zdolność reagowania na takie zagrożenia i ataki poprzez wykorzystanie istniejących zasobów i lepszą koordynację wysiłków. Wszystkie właściwe podmioty w UE muszą być przygotowane do wspólnego reagowania i wymiany informacji na zasadzie „potrzebnego dostępu", a nie „ograniczonego dostępu".

(4) Pomimo znacznych postępów osiągniętych dzięki współpracy między państwami członkowskimi w dziedzinie cyberbezpieczeństwa, w szczególności w ramach grupy współpracy („grupa współpracy NIS") oraz sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) utworzonej na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([2]), nadal nie istnieje wspólna platforma UE, na której można by skutecznie i bezpiecznie wymieniać informacje zgromadzone w różnych społecznościach zajmujących się cyberbezpieczeństwem oraz na której odpowiednie podmioty mogłyby koordynować i mobilizować zdolności operacyjne. Powstaje zatem ryzyko, że cyberzagrożenia i cyberincydenty będą zwalczane w ramach silosów o ograniczonej skuteczności i większej podatności. Ponadto brakuje unijnego kanału współpracy technicznej i operacyjnej z sektorem prywatnym, zarówno w zakresie wymiany informacji, jak i wsparcia reagowania na incydenty.

([1]) ENISA, „2020 Threat Landscape" [Krajobraz zagrożeń 2020]; Europol, „Internet Organised Crime Threat Assessment (IOCTA)" [Ocena zagrożenia wykorzystaniem internetu przez zorganizowane grupy przestępcze (IOCTA)] 2020.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

(5) Istniejące ramy, struktury oraz zasoby i wiedza ekspercka dostępne w państwach członkowskich i właściwych instytucjach, organach i agencjach UE stanowią solidną podstawę wspólnej reakcji na zagrożenia, incydenty i kryzysy związane z cyberbezpieczeństwem ([3]). Po stronie operacyjnej ta istniejąca architektura obejmuje plan skoordynowanego reagowania na wypadek wystąpienia incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych („plan działania") ([4]), sieć CSIRT i europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe") ([5]), a także Europejskie Centrum ds. Walki z Cyberprzestępczością („EC3") oraz Wspólną Grupę Zadaniową ds. Przeciwdziałania Cyberprzestępczości („J-CAT") przy Agencji Unii Europejskiej ds. Współpracy Organów Ścigania („Europol"), jak również unijny protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych („EU LE ERP"). Grupa współpracy NIS, Centrum Analiz Wywiadowczych UE („INTCEN"), zestaw narzędzi dla dyplomacji cyfrowej ([6]) oraz projekty związane z cyberobroną uruchomione w ramach stałej współpracy strukturalnej (PESCO) ([7]) również przyczyniają się do współpracy politycznej i operacyjnej w różnych społecznościach zajmujących się cyberbezpieczeństwem. Na podstawie rozszerzonego mandatu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA") jej zadaniem jest wspieranie współpracy operacyjnej ([8]) w odniesieniu do cyberbezpieczeństwa sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób dotkniętych cyberzagrożeniami i cyberincydentami. Za pomocą zintegrowanych uzgodnień dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) UE jest w stanie koordynować reakcję polityczną na poważne kryzysy, w tym cyberataki na dużą skalę.

(6) Nie istnieje jednak jeszcze mechanizm służący wykorzystaniu istniejących zasobów i zapewnianiu wzajemnej pomocy między społecznościami zajmującymi się cyberbezpieczeństwem odpowiedzialnymi za bezpieczeństwo sieci i systemów informatycznych, walkę z cyberprzestępczością, cyberdyplomację oraz, w stosownych przypadkach, cyberobronę w przypadku kryzysu. Na szczeblu UE nie istnieje również kompleksowy mechanizm współpracy technicznej i operacyjnej między wszystkimi społecznościami w zakresie orientacji sytuacyjnej, gotowości i reagowania. Ponadto synergię z organami ścigania i społecznościami wywiadowczymi należy osiągać odpowiednio za pośrednictwem Europolu i INTCEN.

(7) Komisja, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa („Wysoki Przedstawiciel"), państwa członkowskie oraz właściwe instytucje, organy i agencje UE dostrzegły potrzebę przeprowadzenia analizy mocnych i słabych stron, niedociągnięć i dublowania aspektów obecnej architektury cyberbezpieczeństwa UE, którą utworzono w ostatnich latach. W porozumieniu z państwami członkowskimi Komisja, przy udziale Wysokiego Przedstawiciela, opracowała koncepcję wspólnej jednostki ds. cyberprzestrzeni w odpowiedzi na tę analizę oraz jako ważny element strategii w zakresie unii bezpieczeństwa ([9]), strategii cyfrowej ([10]) i strategii w zakresie cyberbezpieczeństwa ([11]).

([3]) Państwa członkowskie utworzyły europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) w odpowiedzi na zalecenie w sprawie planu działania. Jest to sieć krajowych ekspertów w dziedzinie zarządzania operacyjnego i kryzysowego, sformalizowana w ramach wniosku Komisji z grudnia 2020 r. dotyczącego dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

([4]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

([5]) Zalecenie uwzględnia sprawozdanie z przeprowadzonych działań w odniesieniu do ćwiczenia symulacyjnego w zakresie planu działania na poziomie operacyjnym (Blue OLEx) z 2020 r., a w szczególności przygotowane przez przewodniczącego streszczenie strategicznej dyskusji politycznej na temat wspólnej jednostki ds. cyberprzestrzeni.

([6]) Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej") z dnia 19 czerwca 2017 r. (9916/17).

([7]) W szczególności projekty PESCO dotyczące: „zespołów szybkiego reagowania na cyberincydenty i pomocy wzajemnej w zakresie cyberbezpieczeństwa" (koordynowany przez Litwę) oraz „centrum koordynacji w dziedzinie cyberprzestrzeni i informacji" (koordynowany przez Niemcy).

([8]) Art. 7 rozporządzenia 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) (Dz.U. L 151 z 7.6.2019, s. 15) zobowiązuje Agencję do wspierania współpracy operacyjnej pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz pomiędzy interesariuszami. Obejmuje to wspieranie państw członkowskich w zakresie współpracy operacyjnej w ramach sieci CSIRT, przygotowywanie regularnego szczegółowego raportu technicznego o stanie cyberbezpieczeństwa w UE w odniesieniu do incydentów i cyberzagrożeń oraz wkład w opracowanie wspólnej reakcji na szczeblu Unii i państw członkowskich na transgraniczne incydenty lub kryzysy na dużą skalę. Ponadto ENISA uczestniczy w działaniach szkoleniowych z Europejskim Kolegium Bezpieczeństwa i Obrony (EKBiO).

([9]) Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa, COM(2020) 605 final.

([10]) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Kształtowanie cyfrowej przyszłości Europy, COM(2020) 67 final.

([11]) Wspólny komunikat do Parlamentu Europejskiego i Rady: Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final.

(8) W przypadku kryzysu państwa członkowskie powinny móc polegać na solidarności UE w formie skoordynowanej pomocy, w tym ze strony wszystkich czterech społeczności zajmujących się cyberbezpieczeństwem, tj. społeczności cywilnej, organów ścigania ([12]), dyplomacji i, w stosownych przypadkach, obrony. Stopień interwencji uczestników z jednej lub kilku społeczności może zależeć od charakteru incydentu lub kryzysu na dużą skalę, a w konsekwencji od rodzaju środków przeciwdziałania, które będą wymagane, aby zareagować na ten incydent lub kryzys. W obliczu cyberzagrożeń, cyberincydentów i cyberkryzysów dobrze wyszkoleni eksperci i wyposażenie techniczne stanowią podstawowe aktywa, które mogą przyczynić się do uniknięcia poważnych szkód i do skutecznej odbudowy. Dlatego też priorytetem wspólnej jednostki ds. cyberprzestrzeni będą wyraźnie określone zdolności techniczne i operacyjne gotowe do wykorzystania w państwach członkowskich w razie potrzeby – a przede wszystkim eksperci i sprzęt. W ramach tej platformy uczestnicy będą mieli wyjątkową możliwość rozwoju i koordynacji takich zdolności za pośrednictwem unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa, zapewniając jednocześnie odpowiednią synergię z już istniejącymi projektami w dziedzinie cyberbezpieczeństwa prowadzonymi w ramach PESCO.

(9) Wspólna jednostka ds. cyberprzestrzeni zapewnia wirtualną i fizyczną platformę i nie wymaga utworzenia dodatkowego, samodzielnego organu. Jej ustanowienie nie powinno mieć wpływu na kompetencje i uprawnienia krajowych organów ds. cyberbezpieczeństwa i odpowiednich podmiotów unijnych. Wspólna jednostka ds. cyberprzestrzeni powinna zostać umocowana na podstawie protokołów ustaleń między jej uczestnikami. Powinna ona opierać się na istniejących strukturach, zasobach i zdolnościach i wnosić w nie wkład jako platforma bezpiecznej i szybkiej współpracy operacyjnej i technicznej między podmiotami UE a organami państw członkowskich. Powinna ona również skupiać wszystkie społeczności zajmujące się cyberbezpieczeństwem, tj. społeczność cywilną, organy ścigania, dyplomację i obronę. Uczestnicy platformy powinni pełnić rolę operacyjną lub wspierającą. Uczestnikami operacyjnymi powinny być: ENISA, Europol, zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE („CERT-UE"), Komisja, Europejska Służba Działań Zewnętrznych (w tym INTCEN), sieć CSIRT i EU-CyCLONe. Uczestnikami wspierającymi powinny być: Europejska Agencja Obrony („EDA"), przewodniczący grupy współpracy NIS, przewodniczący Horyzontalnej Grupy Roboczej Rady ds. Cyberprzestrzeni oraz jeden przedstawiciel odpowiednich projektów PESCO ([13]). Ponieważ państwa członkowskie posiadają zdolności operacyjne i kompetencje do reagowania na cyberzagrożenia, cyberincydenty i cyberkryzysy na dużą skalę, uczestnicy platformy powinni polegać przede wszystkim na swoich zdolnościach, z pomocą odpowiednich podmiotów unijnych, aby osiągnąć swoje cele.

(10) Wspólna jednostka ds. cyberprzestrzeni powinna nadać nowy impuls procesowi rozpoczętemu w 2017 r. w planie działania. Powinna ona dodatkowo usprawnić architekturę planu działania i stanowić decydujący krok w kierunku europejskich ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, w których identyfikacja i ograniczanie zagrożeń i ryzyka oraz reagowanie na nie są prowadzone w sposób skoordynowany i terminowy. Czyniąc taki krok, wspólna jednostka ds. cyberprzestrzeni powinna pomóc UE w reagowaniu na obecne i przyszłe zagrożenia.

(11) Dzięki udziałowi we wspólnej jednostce ds. cyberprzestrzeni uczestnicy operacyjni i wspierający powinni mieć możliwość współpracy z szerszą grupą zainteresowanych stron w obrębie unijnych ram reagowania w sytuacji kryzysu cyberbezpieczeństwa. Wykonując funkcje w granicach swoich mandatów, uczestnicy powinni skorzystać ze zwiększonej gotowości i szerszej orientacji sytuacyjnej obejmującej wszystkie aspekty związane z zagrożeniami i incydentami w zakresie cyberbezpieczeństwa, a także z dodatkowej wiedzy fachowej w dziedzinie cyberbezpieczeństwa. Na przykład uczestnicy powinni regularnie angażować się w ćwiczenia między społecznościami, przyjąć jasno określone role w unijnym planie reagowania kryzysowego, zwiększać widoczność swoich działań poprzez wspólną komunikację publiczną oraz zawierać umowy o współpracy operacyjnej z sektorem prywatnym. Jednocześnie wkład we wspólną jednostkę ds. cyberprzestrzeni powinien umożliwić uczestnikom wzmocnienie istniejących sieci, takich jak sieć CSIRT i EU-CyCLONe, oferując im bezpieczne narzędzia wymiany informacji i lepsze zdolności wykrywania (tj. centra monitorowania bezpieczeństwa, „SOC") i umożliwiając korzystanie z dostępnych zdolności operacyjnych UE.

(12) Uczestnicy wspólnej jednostki ds. cyberprzestrzeni powinni skupić się na współpracy technicznej i operacyjnej, w tym na wspólnych operacjach. Uczestnicy powinni przyczyniać się do takiej współpracy w zakresie, w jakim umożliwiają to ich mandaty. Współpraca powinna opierać się na bieżących wysiłkach i uzupełniać je. W zależności od rodzaju współpracy mogą w niej brać udział dodatkowi uczestnicy.

([12]) Również w odniesieniu do współpracy sądowej.

([13]) Zob. przypis 5. ESDZ i EDA, pełniąc rolę sekretariatu PESCO, będą współpracować z koordynatorami odpowiednich projektów PESCO.

(13) Platforma powinna gromadzić ekspertów w dziedzinie technicznego i operacyjnego zarządzania kryzysowego z państw członkowskich oraz podmioty UE w celu koordynacji reagowania na cyberzagrożenia, cyberincydenty i cyberkryzysy dzięki wykorzystaniu istniejących zdolności i wiedzy fachowej. Eksperci uczestniczący we wspólnej jednostce ds. cyberprzestrzeni będą mogli monitorować i chronić znacznie większą powierzchnię ataku dzięki wykorzystaniu platformy fizycznej i wirtualnej. W tym celu uczestnicy powinni korzystać z platformy, aby koordynować wysiłki w przypadku transgranicznych incydentów i kryzysów oraz w przypadku pomocy krajom dotkniętym incydentami.

(14) Stworzenie wspólnej jednostki ds. cyberprzestrzeni wymaga zastosowania stopniowej procedury wykorzystującej i konsolidującej istniejące ramy i struktury, o których mowa w niniejszym zaleceniu, w tym mechanizmy współpracy ustanowione na forach prowadzonych przez państwa członkowskie (np. sieć CSIRT, EU-CyCLONe, Horyzontalna Grupa Robocza Rady ds. Cyberprzestrzeni, J-CAT i odpowiednie projekty PESCO), a ze strony instytucji, organów i agencji UE – ustrukturyzowanej współpracy między ENISA i CERT-UE oraz współpracy z międzyinstytucjonalną grupą wymiany informacji o cyberbezpieczeństwie. Należy odpowiednio uwzględnić ramy zagrożeń hybrydowych, ramy ochrony ludności ([14]) i ramy sektorowe ([15]). Należy też stworzyć ustrukturyzowane powiązanie z IPCR ([16]). W przypadku kryzysu umożliwi to szybkie i skuteczne przekazywanie informacji zgromadzonym w Radzie decydentom na szczeblu politycznym.

(15) Utworzenie wspólnej jednostki ds. cyberprzestrzeni powinno zatem przebiegać zgodnie ze stopniową i przejrzystą procedurą, która zostanie zakończona w ciągu najbliższych dwóch lat. Z tego względu cele określone w niniejszym zaleceniu powinny zostać osiągnięte w drodze czteroetapowej procedury opisanej w załączniku do niniejszego zalecenia. Procedura przygotowawcza, zorganizowana i wspierana przez ENISA, z udziałem uczestników operacyjnych i wspierających na szczeblu UE i państw członkowskich, powinna rozpocząć się na pierwszych dwóch etapach i odbywać się w ramach grupy roboczej, która zostanie utworzona przez Komisję. Prace przygotowawcze powinny opierać się na zasadach wzajemnego zaangażowania, włączenia i budowania konsensusu. Należy wspierać zaangażowanie wszystkich uczestników, umożliwiać wyrażanie różnych poglądów i stanowisk oraz starać się znaleźć rozwiązania, które cieszą się największym poparciem. W zależności od potrzeb i w oparciu o dobrze uzasadnione warunki harmonogram poszczególnych etapów wskazanych w niniejszym zaleceniu może zostać dostosowany.

(16) W ramach pierwszego etapu procedura przygotowawcza powinna rozpocząć się od określenia odpowiednich dostępnych zdolności operacyjnych UE oraz rozpoczęcia oceny ról i obowiązków uczestników platformy. Etap drugi powinien obejmować opracowanie unijnego planu reagowania na incydenty i kryzysy, spójnego z planem działania ([17]) i unijnym protokołem działań w zakresie egzekwowania prawa w sytuacjach kryzysowych, wdrożenie działań związanych z gotowością i orientacją sytuacyjną, zgodnych z aktem o cyberbezpieczeństwie i rozporządzeniem w sprawie Europolu ([18]), a także zakończenie oceny ról i obowiązków uczestników platformy. Grupa robocza powinna przedstawić wyniki tej oceny Komisji i Wysokiemu Przedstawicielowi, którzy następnie przekażą je Radzie. Komisja i Wysoki Przedstawiciel powinni współpracować, zgodnie ze swoimi odpowiednimi kompetencjami, w celu sporządzenia wspólnego sprawozdania na podstawie tej oceny i powinni zwrócić się do Rady o zatwierdzenie tego sprawozdania w drodze konkluzji Rady.

(17) Po tym zatwierdzeniu wspólna jednostka ds. cyberprzestrzeni rozpocznie działanie, z myślą o zakończeniu dwóch pozostałych etapów procedury. W ramach etapu trzeciego uczestnicy powinni mieć możliwość korzystania z unijnych zespołów szybkiego reagowania w ramach wspólnej jednostki ds. cyberprzestrzeni, zgodnie z procedurami określonymi w unijnym planie reagowania na incydenty i kryzysy, wykorzystując zarówno fizyczną, jak i wirtualną platformę i przyczyniając się do różnych aspektów reagowania na incydenty (od komunikacji publicznej po odbudowę *ex post*). W ramach etapu czwartego zainteresowane strony z sektora prywatnego, w tym użytkownicy i dostawcy rozwiązań i usług w zakresie cyberbezpieczeństwa, zostaną zaproszone do wniesienia wkładu w platformę, co umożliwi uczestnikom poprawę wymiany informacji i wzmocnienie skoordynowanej reakcji UE na cyberzagrożenia i cyberincydenty.

([14]) W tym kontekście wspólna jednostka ds. cyberprzestrzeni powinna stworzyć synergię z Unijnym Mechanizmem Ochrony Ludności (UCPM) w celu zwiększenia gotowości i reagowania w Europie w przypadku zbiegu wielu katastrof i sytuacji wyjątkowych, które obejmują element cybernetyczny.

([15]) Jak np. ramy sektora finansowego przewidziane na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/xx* [DORA].

([16]) Zob. motyw 5.

([17]) Zob. przypis 3.

([18]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

(18) Z końcem czteroetapowej procedury uczestnicy powinni sporządzić sprawozdanie z działalności dotyczące postępów w realizacji czterech etapów określonych w zaleceniu, opisujące osiągnięcia i wyzwania, które to sprawozdanie należy przedstawić Komisji i Wysokiemu Przedstawicielowi. Na podstawie tego sprawozdania Komisja i Wysoki Przedstawiciel powinni przeprowadzić ocenę wyników i wyciągnąć wnioski dotyczące przyszłości wspólnej jednostki ds. cyberprzestrzeni.

(19) Komisja, ENISA, Europol i CERT-UE powinny zapewniać wsparcie administracyjne, finansowe i techniczne wspólnej jednostki ds. cyberprzestrzeni zgodnie z sekcją IV niniejszego zalecenia, z zastrzeżeniem dostępności środków budżetowych i zasobów ludzkich. Wzmocnienie zdolności operacyjnych właściwych instytucji, organów i agencji UE w zakresie cyberbezpieczeństwa będzie miało kluczowe znaczenie dla zapewnienia skutecznego przygotowania oraz trwałości wspólnej jednostki ds. cyberprzestrzeni. Komisja zamierza zapewnić, aby przyszłe rozporządzenie w sprawie wspólnych wiążących zasad dotyczących cyberbezpieczeństwa dla instytucji, organów i agencji UE (październik 2021 r.) stanowiło podstawę prawną tego wkładu w odniesieniu do CERT-UE.

(20) W związku ze swoim rozszerzonym mandatem na mocy rozporządzenia (UE) 2019/881 („akt o cyberbezpieczeństwie") ENISA ma wyjątkową możliwość zorganizowania i wspierania przygotowania wspólnej jednostki ds. cyberprzestrzeni, a także przyczynienia się do jej uruchomienia. Zgodnie z przepisami aktu o cyberbezpieczeństwie ENISA tworzy obecnie biuro w Brukseli w celu wspierania zorganizowanej współpracy z CERT-UE. Ta współpraca strukturalna, w tym sąsiadujące biura, zapewni użyteczne ramy ułatwiające utworzenie wspólnej jednostki ds. cyberprzestrzeni, w tym utworzenie fizycznej przestrzeni, która w razie potrzeby powinna być udostępniana uczestnikom, a także pracownikom innych właściwych instytucji, organów i agencji UE. Fizyczną platformę należy połączyć z wirtualną platformą składającą się z narzędzi współpracy i bezpiecznej wymiany informacji. Narzędzia te będą wykorzystywać bogaty zasób informacji gromadzonych za pośrednictwem europejskiej tarczy chroniącej przed zagrożeniami dla cyberbezpieczeństwa ([19]), w tym centrów monitorowania bezpieczeństwa („SOC") oraz ośrodków wymiany i analizy informacji („ISAC").

(21) W przypadku poważnych transgranicznych cyberataków unijny protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych, przyjęty przez Radę w 2018 r., nadaje centralną rolę Europejskiemu Centrum ds. Walki z Cyberprzestępczością („EC3") ([20]) działającemu przy Europolu w ramach planu działania. Protokół ten umożliwia unijnym organom ścigania nieprzerwane reagowanie na ataki transgraniczne na dużą skalę o podejrzewanym złośliwym charakterze dzięki szybkiej reakcji i ocenie oraz bezpiecznej i szybkiej wymianie informacji krytycznych w celu skutecznej koordynacji reagowania na incydenty transgraniczne. Protokół doprecyzowuje współpracę z innymi instytucjami UE i w ramach ogólnounijnych protokołów kryzysowych, a także współpracę kryzysową z sektorem prywatnym. Społeczność organów ścigania, w stosownych przypadkach wspierana przez Europol, powinna wnieść wkład we wspólną jednostkę ds. cyberprzestrzeni, czyniąc niezbędne kroki w ramach pełnego cyklu dochodzenia, zgodnie z wymogami ram wymiaru sprawiedliwości w sprawach karnych i mającymi zastosowanie procedurami przetwarzania dowodów elektronicznych. Europol zapewnia wsparcie operacyjne i ułatwia współpracę operacyjną w zakresie przeciwdziałania cyberzagrożeniom od momentu utworzenia EC3 w 2013 r. Europol powinien wspierać platformę zgodnie ze swoim mandatem i podejściem opartym na działaniach policyjnych z wykorzystaniem danych wywiadowczych, wykorzystując przy tym wszelkiego rodzaju wewnętrzną wiedzę fachową, produkty, narzędzia i usługi mające znaczenie dla reagowania na incydent lub kryzys.

(22) Dyrektywa 2013/40/UE dotycząca ataków na systemy informatyczne wymaga również od państw członkowskich zapewnienia, aby posiadały one funkcjonujący krajowy punkt kontaktowy dostępny 24 godziny na dobę oraz przez siedem dni w tygodniu do celów wymiany informacji dotyczących przestępstw określonych w tej dyrektywie. Sieć funkcjonujących krajowych punktów kontaktowych powinna również wnosić wkład we wspólną jednostkę ds. cyberprzestrzeni, zapewniając w stosownych przypadkach zaangażowanie organów ścigania państw członkowskich.

(23) Unijna społeczność dyplomacji cyfrowej przyczynia się do promowania i ochrony globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni oraz do zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich i reagowania na nie. W 2017 r. UE ustanowiła ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej"). Ramy te są częścią szerszej unijnej polityki dyplomacji cyfrowej. Przyczyniają się do zapobiegania konfliktom i do większej stabilności w stosunkach międzynarodowych. Umożliwiają Unii i państwom członkowskim, w stosownych przypadkach we współpracy z partnerami międzynarodowymi, stosowanie wszystkich środków w ramach wspólnej polityki zagranicznej i bezpieczeństwa („WPZiB"), zgodnie z odpowiednimi procedurami ich osiągnięcia, w celu zachęcania do współpracy, łagodzenia zagrożeń oraz wpływania na obecne i potencjalne przyszłe szkodliwe zachowania w cyberprzestrzeni. Społeczność dyplomacji cyfrowej powinna współpracować w ramach wspólnej jednostki ds. cyberprzestrzeni, stosując i zapewniając wsparcie w stosowaniu pełnego zakresu środków dyplomatycznych, zwłaszcza w zakresie komunikacji publicznej, wspierania wspólnej orientacji sytuacyjnej i współpracy z państwami trzecimi w przypadku kryzysu.

([19]) JOIN(2020) 18 final, sekcja 1.2.
([20]) Ustanowione rozporządzeniem (UE) 2016/794.

(24) Zgodnie z ramami planu działania Wysoki Przedstawiciel, w tym za pośrednictwem INTCEN, powinien wnieść wkład we wspólną jednostkę ds. cyberprzestrzeni, zapewniając stałą, opartą na danych wywiadowczych wspólną orientację sytuacyjną na temat istniejących i pojawiających się zagrożeń, w tym niezbędną strategiczną orientację sytuacyjną w odniesieniu do danego wydarzenia.

(25) W ramach społeczności cyberobrony UE i państwa członkowskie dążą do wzmocnienia zdolności w zakresie cyberobrony i dalszego zwiększenia synergii, koordynacji i współpracy między właściwymi instytucjami, organami i agencjami UE, a także współpracy z państwami członkowskimi i pomiędzy nimi, w tym w odniesieniu do misji i operacji w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO). Społeczność działa w oparciu o zarządzanie międzyrządowe na szczeblu UE, krajowe wojskowe struktury dowodzenia oraz zdolności i zasoby wojskowe lub podwójnego zastosowania. Ze względu na jej odmienny charakter należy stworzyć specjalne interfejsy ze wspólną jednostką ds. cyberprzestrzeni, aby umożliwić wymianę informacji ze społecznością cyberobrony ([21]).

(26) Stała współpraca strukturalna stanowi ramy prawne wprowadzone Traktatem z Lizbony ([22]) i ustanowione w 2017 r. w ramach unijnych. Współpraca strukturalna doprowadziła do powstania szeregu projektów PESCO w dziedzinie cyberbezpieczeństwa, co przyczyniło się do wypełnienia zobowiązania nr 11 ([23]) dotyczącego „zapewapewnienia zwiększenia wysiłków w ramach współpracy w zakresie cyberobrony, takich jak wymiana informacji, szkolenia i wsparcie operacyjne". ESDZ, w tym Sztab Wojskowy UE i EDA, tworzą sekretariat PESCO, który zapewnia pojedynczy punkt kontaktowy w ramach Unii w odniesieniu do wszystkich kwestii PESCO, w tym funkcji wsparcia i koordynacji związanych z projektami PESCO (np. ocena nowych wniosków dotyczących projektów, przygotowywanie sprawozdań z postępów projektów itp.). Przedstawiciele odpowiednich projektów PESCO powinni wspierać wspólną jednostkę ds. cyberprzestrzeni, zwłaszcza w odniesieniu do orientacji sytuacyjnej i gotowości.

(27) Za pośrednictwem wspólnej jednostki ds. cyberprzestrzeni uczestnicy powinni odpowiednio integrować zainteresowane strony z sektora prywatnego, w tym dostawców i użytkowników rozwiązań i usług w zakresie cyberbezpieczeństwa, aby wspierać europejskie ramy zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa, uwzględniając odpowiednio ramy prawne dotyczące wymiany danych i bezpieczeństwa informacji. Dostawcy cyberbezpieczeństwa powinni wnieść wkład w tę inicjatywę, dzieląc się informacjami na temat zagrożeń i zapewniając służby reagowania na incydenty w celu szybkiego zwiększenia zdolności jednostki do reagowania na ataki i kryzysy na dużą skalę. Użytkownicy wyrobów i usług związanych z cyberbezpieczeństwem, przede wszystkim ci objęci zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji, powinni mieć możliwość zwracania się o pomoc i doradztwo za pośrednictwem brakujących obecnie ustrukturyzowanych kanałów powiązanych z ośrodkami wymiany i analizy informacji na poziomie UE (ISAC) ([24]). Platforma mogłaby również przyczynić się do zacieśnienia współpracy z partnerami międzynarodowymi.

(28) Rozwijanie i utrzymywanie orientacji sytuacyjnej wymaga najnowocześniejszych zdolności w zakresie wykrywania włamań i zapobiegania im. Wspólna jednostka ds. cyberprzestrzeni powinna opierać się na nowoczesnej sieci zdolnej do analizowania złośliwych zagrożeń i incydentów, które mogą mieć wpływ na kluczowe systemy teleinformatyczne w całej Unii. Oznacza to, że wiedza o zagrożeniach pozyskana m.in. z sieci komunikacyjnych monitorowanych przez centra monitorowania bezpieczeństwa na szczeblu krajowym, sektorowym i transgranicznym powinna być dostarczana wspólnej jednostce ds. cyberprzestrzeni w celu poprawy oceny krajobrazu zagrożeń w UE przez uczestników.

(29) Aby wspierać wymianę informacji operacyjnych, w tym materiałów poufnych, platforma powinna opierać się na odpowiednio bezpiecznych kanałach komunikacji. Takie kanały mogłyby również opierać się na istniejącej infrastrukturze, takiej jak aplikacja sieci bezpiecznej wymiany informacji („SIENA") wykorzystywana przez Europol i organy ścigania. Jak zapowiedziano w strategii w zakresie cyberbezpieczeństwa, narzędzia stosowane przez instytucje, organy i agencje UE powinny być zgodne z przepisami dotyczącymi bezpieczeństwa informacji, które Komisja wkrótce zaproponuje.

([21]) W szczególności poprzez reprezentację ESDZ, aby umożliwić odpowiedni udział społeczności cyberobrony, który opiera się na dobrowolnych wkładach krajowych.

([22]) Art. 42 ust. 6, art. 46 i protokół nr 10 do TUE.

([23]) Każde z państw członkowskich uczestniczących w PESCO podejmuje 20 indywidualnych zobowiązań podzielonych na pięć kluczowych obszarów określonych w art. 2 protokołu nr 10 w sprawie PESCO załączonego do Traktatu o Unii Europejskiej.

([24]) Godne uwagi przykłady istniejących ośrodków ISAC, które mogłyby być zaangażowane w taką wymianę informacji, obejmują ISAC ds. europejskiego sektora energii (EE-ISAC) lub ISAC ds. europejskich instytucji finansowych (FI-ISAC).

(30) Komisja, przede wszystkim za pośrednictwem programu „Cyfrowa Europa", będzie wspierać inwestycje niezbędne do utworzenia fizycznej i wirtualnej platformy oraz budowy i utrzymania bezpiecznych kanałów komunikacji i zdolności szkoleniowych, a także do rozwijania i wdrażania zdolności wykrywania. Ponadto Europejski Fundusz Obronny mógłby pomóc w finansowaniu kluczowych technologii cyberobrony i zdolności w zakresie cyberobrony, co wzmocniłoby krajową gotowość w tym zakresie,

PRZYJMUJE NINIEJSZE ZALECENIE:

I. **CEL ZALECENIA**

1. Celem zalecenia jest określenie działań niezbędnych w celu koordynacji wysiłków UE na rzecz zapobiegania cyberincydentom i cyberkryzysom na dużą skalę, wykrywania ich, zniechęcania do nich, powstrzymywania ich, łagodzenia ich skutków i reagowania na nie za pośrednictwem wspólnej jednostki ds. cyberprzestrzeni. Aby osiągnąć ten cel, w zaleceniu zdefiniowano również procedurę, cele pośrednie i harmonogram, które państwa członkowskie i właściwe instytucje, organy i agencje UE powinny stosować, mając na uwadze stworzenie i rozwój platformy.

2. W przypadku cyberincydentów i kryzysów cyberbezpieczeństwa na dużą skalę państwa członkowskie i właściwe instytucje, ograny i agencje UE powinny zapewnić koordynację wysiłków za pośrednictwem wspólnej jednostki ds. cyberprzestrzeni, która umożliwia wzajemną pomoc ([25]) dzięki wiedzy fachowej organów państw członkowskich i właściwych instytucji, organów i agencji UE. Wspólna jednostka ds. cyberprzestrzeni powinna również umożliwiać uczestnikom współpracę z sektorem prywatnym.

II. **DEFINICJE**

3. Do celów niniejszego zalecenia:

a) „unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa" oznacza zestawienie ról, warunków i procedur prowadzących do utworzenia unijnych ram reagowania w sytuacji kryzysu cyberbezpieczeństwa opisanych w pkt 1 zalecenia Komisji z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („plan działania");

b) „społeczności zajmujące się cyberbezpieczeństwem" oznaczają współpracujące grupy cywilne, organów ścigania, dyplomacji i obrony reprezentujące zarówno państwa członkowskie, jak i właściwe instytucje, organy i agencje UE, które wymieniają się informacjami, dążąc do osiągnięcia wspólnych celów, interesów i misji związanych z cyberbezpieczeństwem;

c) „uczestnicy sektora prywatnego" oznaczają przedstawicieli podmiotów sektora prywatnego dostarczających lub stosujących rozwiązania ([26]) i usługi ([27]) w zakresie cyberbezpieczeństwa;

d) „incydent na dużą skalę" oznacza incydent zdefiniowany w art. 4 pkt 7 dyrektywy (UE) 2016/1148, mający znaczący wpływ w co najmniej w dwóch państwach członkowskich;

e) „zintegrowany raport o stanie cyberbezpieczeństwa w UE" oznacza sprawozdanie gromadzące informacje od uczestników wspólnej jednostki ds. cyberprzestrzeni, oparte na raporcie technicznym o stanie cyberbezpieczeństwa w UE określonym w art. 7 ust. 6 rozporządzenia (UE) 2019/881;

f) „unijny zespół szybkiego reagowania w dziedzinie cyberbezpieczeństwa" oznacza zespół złożony z uznanych ekspertów w dziedzinie cyberbezpieczeństwa, w szczególności z CSIRT państw członkowskich, przy wsparciu ze strony ENISA, CERT-UE i Europolu, który jest gotowy do zdalnej pomocy uczestnikom, których dotyczą incydenty i kryzysy na dużą skalę;

g) „protokół ustaleń" oznacza porozumienie między uczestnikami określające niezbędne warunki współpracy, w tym definicję zasobów i procedur niezbędnych do utworzenia i zmobilizowania unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa, a także umożliwiające wzajemną pomoc.

([25]) Spójnie z podejściem i zasadami określonymi w dyrektywie (UE) 2016/1148 i w art. 222 TFUE. Bez uszczerbku dla art. 42 ust. 7 Traktatu o Unii Europejskiej.
([26]) W tym sprzedawcy oprogramowania.
([27]) W tym dane wywiadowcze na temat zagrożeń.

III. CEL WSPÓLNEJ JEDNOSTKI DS. CYBERPRZESTRZENI

4. Państwa członkowskie oraz właściwe instytucje, organy i agencje UE powinny zapewnić **skoordynowaną reakcję UE** na cyberincydenty i cyberkryzysy na dużą skalę oraz odbudowę w ich następstwie. W szczególności należy zapewnić taką reakcję pomiędzy uczestnikami operacyjnymi, zwłaszcza ENISA, Europolem, CERT-UE, Komisją, Europejską Służbą Działań Zewnętrznych (w tym INTCEN), siecią CSIRT, EU-CyCLONe, a uczestnikami wspierającymi, zwłaszcza przewodniczącym grupy współpracy NIS, przewodniczącym Horyzontalnej Grupy Roboczej Rady ds. Cyberprzestrzeni, Europejską Agencją Obrony i jednym przedstawicielem odpowiednich projektów PESCO ([28]). Uczestnicy operacyjni powinni być w stanie szybko i skutecznie mobilizować zasoby operacyjne na potrzeby wzajemnej pomocy w ramach wspólnej jednostki ds. cyberprzestrzeni. W tym celu w ramach wspólnej jednostki ds. cyberprzestrzeni należy koordynować mechanizmy wzajemnej pomocy na wniosek jednego lub większej liczby państw członkowskich.

5. Aby zapewnić skuteczną i skoordynowaną reakcję, uczestnicy operacyjni i wspierający, wymienieni w pkt 4, powinni mieć możliwość dzielenia się najlepszymi praktykami, korzystania z ciągłej **wspólnej orientacji sytuacyjnej** oraz zapewnienia niezbędnej **gotowości** w zakresie dozwolonym przez ich mandaty. Uczestnicy ci powinni uwzględniać istniejące procedury i wiedzę fachową różnych społeczności zajmujących się cyberbezpieczeństwem.

IV. DEFINIOWANIE FUNKCJONOWANIA WSPÓLNEJ JEDNOSTKI DS. CYBERPRZESTRZENI

6. Państwa członkowskie oraz właściwe instytucje, organy i agencje UE, w oparciu o wkład ENISA zgodnie z art. 7 ust. 7 rozporządzenia (UE) 2019/881, powinny zapewnić **skoordynowaną reakcję** na incydenty i kryzysy na dużą skalę oraz odbudowę po nich poprzez:

a) utworzenie, szkolenie, testowanie i skoordynowane wykorzystanie **unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa** w oparciu o art. 7 ust. 4 rozporządzenia (UE) 2019/881 oraz art. 3 i 4 rozporządzenia (UE) 2016/794;

b) skoordynowane wdrożenie **wirtualnej i fizycznej platformy** wykorzystującej współpracę strukturalną ENISA i CERT-UE przewidzianą w art. 7 ust. 4 rozporządzenia (UE) 2019/881, która powinna służyć jako infrastruktura wspierająca współpracę techniczną i operacyjną między uczestnikami oraz być wykorzystywana w celu gromadzenia odpowiedniego personelu i innych zasobów oferowanych przez uczestników;

c) utworzenie i utrzymywanie wykazu **zdolności operacyjnych i technicznych dostępnych w UE** we wszystkich społecznościach zajmujących się cyberbezpieczeństwem ([29]) w Unii, które są gotowe do wykorzystania w przypadku cyberincydentów lub kryzysów cyberbezpieczeństwa na dużą skalę;

d) sprawozdawczość na rzecz Komisji i Wysokiego Przedstawiciela na temat doświadczeń zdobytych w ramach **współpracy operacyjnej w dziedzinie cyberbezpieczeństwa** w społecznościach zajmujących się cyberbezpieczeństwem i między nimi.

7. Państwa członkowskie oraz właściwe instytucje, organy i agencje UE powinny zapewnić, aby wspólna jednostka ds. cyberprzestrzeni oferowała stałą wspólną **orientację sytuacyjną** i **gotowość** na wypadek cyberkryzysów we wszystkich społecznościach zajmujących się cyberbezpieczeństwem, a także w obrębie tych społeczności, realizując cele określone w art. 7 rozporządzenia (UE) 2019/881 i art. 3 rozporządzenia (UE) 2016/794. W tym celu państwa członkowskie oraz właściwe instytucje, organy i agencje UE, zgodnie z rozporządzeniem (UE) 2019/881 i rozporządzeniem (UE) 2016/794, powinny umożliwić realizację następujących operacji **wspierających**:

a) opracowanie **zintegrowanego raportu o stanie cyberbezpieczeństwa w UE** poprzez gromadzenie i analizowanie wszystkich istotnych informacji i danych wywiadowczych dotyczących zagrożeń;

b) wykorzystanie odpowiednich i bezpiecznych **narzędzi**, zgodnie z art. 7 ust. 1 rozporządzenia (UE) 2019/881, służących do szybkiej wymiany informacji między uczestnikami i innymi podmiotami;

c) **wymiana informacji i wiedzy fachowej** niezbędnych do przygotowania Unii do zarządzania cyberincydentami i cyberkryzysami na dużą skalę, przy wsparciu ENISA, jak określono w art. 7 ust. 2 rozporządzenia (UE) 2019/881;

d) przyjęcie i testowanie krajowych **planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa** ([30]) zgodnie z art. 7 ust. 2, 5 i 7 rozporządzenia (UE) 2019/881;

([28]) „Centrum koordynacji działań w zakresie cyberprzestrzeni i informacji" (CIDCC) oraz „zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa" (CRRT).

([29]) W tym, w stosownych przypadkach, społeczność cyberobrony.

([30]) Proponowane na mocy art. 7 ust. 3 dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

e) opracowanie **unijnego planu reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa**, zarządzanie nim i testowanie go, w tym poprzez ćwiczenia i szkolenia między społecznościami, zgodnie z zaleceniem w sprawie planu działania i w oparciu o art. 7 ust. 3 wniosku Komisji dotyczącego przeglądu dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii ([31]);

f) pomoc uczestników w zawieraniu umów o wymianie informacji, a także umów o współpracy operacyjnej z **podmiotami sektora prywatnego** świadczącymi m.in. usługi wywiadowcze w zakresie zagrożeń i usługi reagowania na incydenty, przy wsparciu ENISA, jak określono w art. 7 ust. 1 rozporządzenia (UE) 2019/881;

g) ustanowienie ustrukturyzowanych synergii z krajowymi, sektorowymi i transgranicznymi **zdolnościami w zakresie monitorowania i wykrywania**, w szczególności z centrami monitorowania bezpieczeństwa;

h) pomoc uczestników w **zarządzaniu** incydentami i kryzysami na dużą skalę, zgodnie ze wspierającą rolą ENISA określoną w art. 7 rozporządzenia (UE) 2019/881. Obejmuje to wnoszenie wkładu we wspólną orientację sytuacyjną, wspieranie działań dyplomatycznych, podział zadań w odniesieniu do polityki i dochodzeń w sprawach karnych, w tym za pośrednictwem Europolu ([32]), koordynację komunikacji publicznej i ułatwianie odbudowy w wyniku incydentów.

8. W celu wdrożenia pkt 6 i 7 państwa członkowskie oraz właściwe instytucje, organy i agencje UE powinny zapewnić:

a) określenie aspektów organizacyjnych wspólnej jednostki ds. cyberprzestrzeni oraz **ról i obowiązków** uczestników operacyjnych i wspierających w ramach platformy, co umożliwi skuteczne funkcjonowanie platformy zgodnie z aspektami i zasadami określonymi w załączniku do niniejszego zalecenia;

b) zawarcie **protokołów ustaleń** określających niezbędne warunki współpracy między uczestnikami, o których mowa w pkt 4.

9. Zgodnie z art. 7 rozporządzenia (UE) 2019/881 ENISA powinna zapewnić koordynację i wsparcie państw członkowskich oraz właściwych instytucji, agencji i organów UE w ramach wspólnej jednostki ds. cyberprzestrzeni, w tym poprzez pełnienie roli sekretariatu, organizowanie spotkań i przyczynianie się do realizacji działań zarówno na szczeblu państw członkowskich, jak i UE. ENISA powinna stworzyć zarówno bezpieczną platformę wirtualną, jak i przestrzeń fizyczną, aby organizować spotkania i ułatwiać niezbędne działania wykonawcze.

V. **UTWORZENIE WSPÓLNEJ JEDNOSTKI DS. CYBERPRZESTRZENI**

10. Państwa członkowskie oraz właściwe instytucje, organy i agencje UE powinny zapewnić rozpoczęcie fazy operacyjnej wspólnej jednostki ds. cyberprzestrzeni od dnia **30 czerwca 2022 r.** Do tego czasu uczestnicy operacyjni powinni udostępnić zdolności operacyjne i ekspertów, aby stworzyć podstawę unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa. Plany dotyczące fizycznej i wirtualnej platformy powinny być zaawansowane.

11. Państwa członkowskie oraz właściwe instytucje, organy i agencje UE powinny przyczyniać się do funkcjonowania wspólnej jednostki ds. cyberprzestrzeni i zapewnić jej pełną operacyjność **do dnia 30 czerwca 2023 r.** Należy tego dokonać w czterech kolejnych etapach, które będą miały na celu zakończenie następujących działań:

a) etap pierwszy – ocena aspektów organizacyjnych wspólnej jednostki ds. cyberprzestrzeni i określenie dostępnych zdolności operacyjnych UE do dnia **31 grudnia 2021 r.**;

b) etap drugi – przygotowanie planów reagowania na incydenty i kryzysy oraz rozpoczęcie wspólnych działań w zakresie gotowości do dnia **30 czerwca 2022 r.**;

c) etap trzeci – uruchomienie wspólnej jednostki ds. cyberprzestrzeni do dnia **31 grudnia 2022 r.**;

d) etap czwarty – rozszerzenie współpracy w ramach wspólnej jednostki ds. cyberprzestrzeni na podmioty prywatne i złożenie sprawozdania z poczynionych postępów do dnia **30 czerwca 2023 r.**

Bardziej szczegółowe działania, które należy podjąć w ramach czterech kolejnych etapów, przedstawiono w załączniku do niniejszego zalecenia.

([31]) COM(2020) 823 final.
([32]) Zgodnie z rozporządzeniem (UE) 2016/794.

12. W ramach dwóch pierwszych etapów ENISA powinna zorganizować i wspierać przygotowanie wspólnej jednostki ds. cyberprzestrzeni. Służby Komisji powinny zwołać grupę roboczą skupiającą uczestników operacyjnych i wspierających w celu zakończenia takich prac przygotowawczych. Służby Komisji powinny wyznaczyć przedstawiciela na współprzewodniczącego grupy roboczej i zaprosić do pełnienia funkcji współprzewodniczących: przedstawiciela wyznaczonego przez Wysokiego Przedstawiciela (każdy z nich wnosi wkład do punktów porządku obrad zgodnie z ich odpowiednimi kompetencjami) oraz przedstawiciela wybranego przez państwa członkowskie.

13. Pod koniec etapu drugiego grupa robocza powinna zakończyć ocenę aspektów organizacyjnych wspólnej jednostki ds. cyberprzestrzeni oraz roli i obowiązków uczestników operacyjnych w ramach tej platformy. Grupa robocza powinna przedstawić wyniki tej oceny Komisji i Wysokiemu Przedstawicielowi. Komisja i Wysoki Przedstawiciel powinni następnie przekazać taką ocenę Radzie. Na podstawie tej oceny Komisja i Wysoki Przedstawiciel powinni sporządzić wspólne sprawozdanie i zwrócić się do Rady o jego zatwierdzenie w drodze konkluzji Rady.

14. Wspólna jednostka ds. cyberprzestrzeni powinna zacząć działać od etapu trzeciego.

15. ENISA i Komisja powinny zapewnić wykorzystanie istniejących zasobów w ramach unijnych programów finansowania, przede wszystkim programu „Cyfrowa Europa", zgodnie z obowiązującymi przepisami dotyczącymi ustanawiania odpowiednich programów prac, w celu zapewnienia uczestnikom wspólnej jednostki ds. cyberprzestrzeni dodatkowych zdolności szkoleniowych, zdolności komunikacyjnych i bezpiecznej infrastruktury wymiany informacji umożliwiającej wymianę informacji niejawnych, w tym między społecznościami.

VI. **PRZEGLĄD**

16. Państwa członkowskie powinny współpracować z Komisją i Wysokim Przedstawicielem, zgodnie z ich odpowiednimi kompetencjami, w celu dokonania oceny skuteczności i wydajności wspólnej jednostki ds. cyberprzestrzeni do dnia **30 czerwca 2025 r.** z myślą o wyciągnięciu wniosków dotyczących przyszłości wspólnej jednostki ds. cyberprzestrzeni. Ocena ta powinna uwzględniać realizację wyżej wymienionych czterech etapów.

Sporządzono w Brukseli dnia 23 czerwca 2021 r.

W imieniu Komisji
Thierry BRETON
Członek Komisji

ZAŁĄCZNIK

Etapy tworzenia wspólnej jednostki ds. cyberprzestrzeni

W niniejszym załączniku opisano podstawowe i wspierające działania niezbędne do ustanowienia i uruchomienia wspólnej jednostki ds. cyberprzestrzeni.

1. *Etap 1 – Ocena aspektów organizacyjnych wspólnej jednostki ds. cyberprzestrzeni i określenie dostępnych zdolności operacyjnych UE*

GŁÓWNE DZIAŁANIA

Uczestnicy operacyjni wspólnej jednostki ds. cyberprzestrzeni, zebrani w ramach grupy roboczej powołanej przez Komisję i przy wsparciu ENISA, powinni gromadzić informacje na temat istniejących zdolności operacyjnych, łącznie z wykazem dostępnych uznanych specjalistów ze wskazaniem ich odpowiedniej wiedzy fachowej, i na temat narzędzi, funkcji i aktywów dostępnych na wypadek incydentów oraz dostępnych portfeli szkoleń i ćwiczeń, a także istniejących wyników analizy informacji i danych wywiadowczych. W oparciu o ten wkład uczestnicy operacyjni powinni przygotować **wykaz dostępnych zdolności operacyjnych UE** gotowych do uruchomienia w przypadku cyberincydentów lub cyberkryzysów, w szczególności za pośrednictwem unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa.

Grupa robocza powinna rozpocząć ocenę **aspektów organizacyjnych** wspólnej jednostki ds. cyberprzestrzeni oraz **roli i obowiązków uczestników operacyjnych w ramach tej platformy**.

Aby uzyskać przegląd zdolności i uzgodnić procedury, główne oraz – w miarę możliwości – wspierające działania w ramach pierwszego etapu powinny zostać zakończone do dnia **31 grudnia 2021 r. [6 miesięcy po przyjęciu]**.

2. *Etap 2 – Przygotowanie planów reagowania na incydenty i kryzysy oraz rozpoczęcie wspólnych działań w zakresie gotowości*

GŁÓWNE DZIAŁANIA

Uczestnicy operacyjni w ramach grupy roboczej, w porozumieniu z uczestnikami wspierającymi, powinni przygotować **unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa** na podstawie krajowych planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa. Unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa powinien obejmować cele w zakresie gotowości UE, zidentyfikowane procedury i bezpieczne kanały wymiany informacji, w tym sposoby postępowania z informacjami, a także kryteria uruchomienia mechanizmu wzajemnej pomocy w oparciu o uzgodnioną klasyfikację incydentów oraz wykaz dostępnych zdolności UE.

Pod koniec etapu drugiego grupa robocza powinna zakończyć ocenę aspektów organizacyjnych wspólnej jednostki ds. cyberprzestrzeni oraz roli i obowiązków uczestników operacyjnych w ramach tej platformy. Grupa robocza powinna przedstawić wyniki tej oceny Komisji i Wysokiemu Przedstawicielowi. Komisja i Wysoki Przedstawiciel powinni przedłożyć tę ocenę Radzie. Komisja i Wysoki Przedstawiciel powinni współpracować, zgodnie ze swoimi odpowiednimi kompetencjami, w celu sporządzenia wspólnego sprawozdania na podstawie tej oceny i powinni zwrócić się do Rady o zatwierdzenie tego sprawozdania w drodze konkluzji Rady.

DZIAŁANIA WSPIERAJĄCE

Unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa powinien opierać się na głównych elementach krajowych planów reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa. Zgodnie z wnioskiem Komisji dotyczącym dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 ([1]), państwa członkowskie powinny przyjąć krajowe plany reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa. W planach krajowych, które mogą być ewentualnie przedmiotem wzajemnej oceny, należy określić cele i sposoby zarządzania cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę. Plany krajowe powinny w szczególności obejmować następujące kwestie:

a. cele krajowych środków i działań służących zapewnieniu gotowości;

b. role i obowiązki właściwych organów krajowych na szczeblu krajowym;

c. krajowe procedury zarządzania kryzysowego oraz kanały wymiany informacji;

d. określenie środków służących zapewnieniu gotowości, w tym ćwiczeń i działań szkoleniowych;

e. określenie odpowiednich zaangażowanych zainteresowanych stron publicznych i prywatnych oraz odpowiedniej infrastruktury publicznej i prywatnej;

f. krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi, w tym organami i instytucjami odpowiedzialnymi za wszystkie społeczności zajmujące się cyberbezpieczeństwem, mające na celu zapewnienie skutecznego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę na szczeblu Unii oraz skutecznego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Wykorzystując wkład zapewniony przez państwa członkowskie oraz instytucje, organy i agencje UE, uczestnicy operacyjni powinni przeprowadzić następujące działania wspierające w ramach wspólnej jednostki ds. cyberprzestrzeni:

a. sporządzenie pierwszego zintegrowanego raportu o stanie cyberbezpieczeństwa w UE w oparciu o krajowe plany reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa;

([1]) COM(2020) 823 final, 2020/0359 (COD), Bruksela, 16.12.2020.

b. ustanowienie zdolności komunikacyjnych i bezpiecznych narzędzi wymiany informacji;

c. ułatwienie przyjęcia protokołów dotyczących wzajemnej pomocy między uczestnikami;

d. organizacja obejmujących wszystkie społeczności ćwiczeń i szkoleń dla ekspertów figurujących w wykazie dostępnych zdolności operacyjnych UE;

e. opracowanie wieloletniego planu koordynacji ćwiczeń.

W razie potrzeby uczestnicy operacyjni powinni konsultować się z uczestnikami wspierającymi. ENISA, przy wsparciu Komisji, Europolu i CERT-UE, powinna umożliwiać wymianę informacji poprzez ustanowienie zdolności komunikacyjnych i bezpiecznych narzędzi wymiany informacji.

Aby zapewnić opracowanie niezbędnych planów i rozpoczęcie wspólnych działań, główne oraz – w miarę możliwości – wspierające działania w ramach etapu drugiego powinny zostać zakończone do dnia **30 czerwca 2022 r. [6 miesięcy po zakończeniu etapu 1]**.

3. *Etap 3 – Uruchomienie wspólnej jednostki ds. cyberprzestrzeni*

GŁÓWNE DZIAŁANIA

Po zatwierdzeniu przez Radę wniosków Komisji na temat raportu sporządzonego podczas etapu drugiego uczestnicy operacyjni powinni koordynować wprowadzenie **unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa** w ramach wspólnej jednostki ds. cyberprzestrzeni oraz ustanowić fizyczną platformę umożliwiającą tymże zespołom realizację działań technicznych i operacyjnych. W oparciu o prace przygotowawcze przeprowadzone w ramach etapu drugiego uczestnicy powinni sfinalizować unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa. Uczestnicy operacyjni powinni upewnić się co do faktycznej dostępności ekspertów i zdolności figurujących w wykazie dostępnych zdolności operacyjnych UE oraz ich gotowości do wniesienia wkładu w działalność unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa.

W celu wdrożenia unijnego planu reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa uczestnicy powinni określić roczny program prac.

DZIAŁANIA WSPIERAJĄCE

Wspólna jednostka ds. cyberprzestrzeni może być wykorzystywana przez społeczność dyplomacji cyfrowej w celu koordynacji komunikacji publicznej. Platforma ta może umożliwić uczestnikom wniesienie wkładu w podział zadań zarówno w odniesieniu do polityki, jak i w przyjęty na szczeblu policyjnym i sądowym podział zadań w ramach wymiaru sprawiedliwości w sprawach karnych. Ponadto może ona ułatwiać odbudowę prawidłowego funkcjonowania i umożliwiać ustrukturyzowaną synergię z krajowymi i transgranicznymi zdolnościami w zakresie monitorowania i wykrywania.

Aby zapewnić uruchomienie wspólnej jednostki ds. cyberprzestrzeni, główne oraz – w miarę możliwości – wspierające działania w ramach etapu trzeciego powinny zostać zakończone do dnia **31 grudnia 2022 r. [6 miesięcy po zakończeniu etapu 2]**.

4. *Etap 4 – Rozszerzenie współpracy w ramach wspólnej jednostki ds. cyberprzestrzeni na podmioty prywatne i złożenie sprawozdania z poczynionych postępów*

GŁÓWNE DZIAŁANIE

Uczestnicy wspólnej jednostki ds. cyberprzestrzeni powinni sporządzić **sprawozdanie** z działalności **dotyczące postępów w realizacji czterech etapów określonych w zaleceniu, opisujące osiągnięcia i napotkane wyzwania**. Sprawozdanie to powinno zawierać informacje statystyczne dotyczące działań w zakresie współpracy operacyjnej prowadzonych na wszystkich czterech etapach. Sprawozdanie należy przedłożyć Komisji i Wysokiemu Przedstawicielowi.

DZIAŁANIA WSPIERAJĄCE

Aby poszerzyć zdolności i informacje dostępne dla unijnych zespołów szybkiego reagowania w dziedzinie cyberbezpieczeństwa, uczestnicy powinni zapewnić, aby wspólna jednostka ds. cyberprzestrzeni pomagała w zawieraniu **umów o wymianie informacji i współpracy operacyjnej między uczestnikami a podmiotami sektora prywatnego** świadczącymi między innymi usługi w zakresie rozpoznania zagrożeń i reagowania na incydenty. W ramach prowadzonych działań powinni oni również zapewnić, by wspólna jednostka ds. cyberprzestrzeni wspierała działania w zakresie regularnego dialogu i wymiany informacji na temat zagrożeń i słabych punktów z użytkownikami rozwiązań w dziedzinie cyberbezpieczeństwa – przede wszystkim tymi objętymi zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji lub zgromadzonymi w **ośrodkach wymiany i analizy informacji na poziomie UE (ISAC)**.

Państwa członkowskie powinny wspierać podmioty działające na ich terytorium, w szczególności podmioty objęte zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji, w dostępie do dialogów publiczno-prywatnych z ISAC na poziomie UE oraz we wkładzie w te dialogi.

Aby zapewnić właściwe zaangażowanie sektora prywatnego, główne oraz – w miarę możliwości – wspierające działania w ramach etapu czwartego powinny zostać zakończone do dnia **30 czerwca 2023 r. [6 miesięcy po zakończeniu etapu 3]**.

JAK SZYBKO URUCHOMIĆ ZDOLNOŚCI OPERACYJNE UE?

KTO ZAPEWNIA ZDOLNOŚCI: Uczestnicy operacyjni

KTO ZARZĄDZA ZDOLNOŚCIAMI: Uczestnicy, w ramach wspólnej jednostki ds. cyberprzestrzeni, zgodnie z ustalonymi rolami i obowiązkami

Etap	Cel	Zadanie	Główne działanie	Działanie wspierające
Etap 1 – określenie do dnia **31 grudnia 2021 r. [6 miesięcy po przyjęciu]**	GOTOWOŚĆ	**Określenie zdolności**	**Uczestnicy operacyjni określają wykaz dostępnych zdolności operacyjnych UE**	
Etap 2 – przygotowanie do dnia **30 czerwca 2022 r. [6 miesięcy po zakończeniu etapu 1]**	GOTOWOŚĆ	**Określenie odpowiednich procedur i rozwiązań w celu uruchomienia zdolności w razie potrzeby**	**Uczestnicy operacyjni przygotowują unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa (unijne ramy reagowania w sytuacji kryzysu cyberbezpieczeństwa, w ramach planu działania), w oparciu o przyjęte plany krajowe**	**Uczestnicy operacyjni opracowują zintegrowane raporty o stanie cyberbezpieczeństwa w UE w oparciu o raport techniczny o stanie cyberbezpieczeństwa w UE**
	GOTOWOŚĆ	**Zdolności ćwiczeniowe**		**Uczestnicy organizują wspólne ćwiczenia i szkolenia (obejmujące wszystkie społeczności)** **Uczestnicy opracowują wieloletni plan koordynacji ćwiczeń**
	ORIENTACJA SYTUACYJNA	**Ustanowienie narzędzi do wymiany informacji i składania wniosków o wsparcie**		**Uczestnicy opracowują bezpieczną i szybką wymianę informacji**
WSPÓLNA JEDNOSTKA DS. CYBERPRZESTRZENI DZIAŁA w oparciu o prace przygotowawcze przeprowadzone przez uczestników w ramach grupy roboczej, którą powołuje Komisja				
Etap 3 – uruchomienie do dnia **31 grudnia 2022 r. [6 miesięcy po zakończeniu etapu 2]**	GOTOWOŚĆ	**Przyjęcie odpowiednich procedur, rozwiązań i protokołów ustaleń w celu uruchomienia zdolności w razie potrzeby**	**Uczestnicy operacyjni finalizują unijny plan reagowania na cyberincydenty i kryzysy cyberbezpieczeństwa i określają jego realizację za pomocą rocznych programów prac**	**Uczestnicy wspierają ustanowienie krajowych i transgranicznych zdolności w zakresie monitorowania i wykrywania, w tym tworzenie SOC (centrów monitorowania bezpieczeństwa)**
	SKOORDYNOWANE REAGOWANIE	**Uruchomienie zdolności w razie potrzeby**	**Uczestnicy operacyjni koordynują działające unijne zespoły szybkiego reagowania w dziedzinie cyberbezpieczeństwa za pośrednictwem wirtualnej i fizycznej platformy wspólnej jednostki ds. cyberbezpieczeństwa w Brukseli**	**Uczestnicy koordynują komunikację publiczną i wnoszą wkład w podział zadań zarówno w odniesieniu do polityki, jak i w ramach wymiaru sprawiedliwości w sprawach karnych**

Etap 4 – Rozszerzenie i sprawozdawczość do dnia **30 czerwca 2023 r. [6 miesięcy po zakończeniu etapu 3]**	ORIENTACJA SYTUACYJNA SKOORDYNOWANE REAGOWANIE	**Zapewnienie skalowalności poprzez zaangażowanie sektora prywatnego w zaspokajanie powstających potrzeb**	**Uczestnicy składają sprawozdanie z działalności dotyczące poczynionych postępów i opisujące osiągnięcia i wyzwania przy pomocy informacji statystycznych**	**Uczestnicy zawierają umowy o wymianie informacji oraz umowy o współpracy operacyjnej z dostawcami rozwiązań w zakresie cyberbezpieczeństwa** **Uczestnicy zawierają umowy o wymianie informacji z użytkownikami rozwiązań w zakresie cyberbezpieczeństwa, przede wszystkim z podmiotami objętymi zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz ISAC działającymi na poziomie UE**