Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wspólny komunikat do Parlamentu Europejskiego i Rady »Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę«"

[JOIN(2020) 18 final]

(2021/C 286/14)

Sprawozdawca: **Philip VON BROCKDORFF**

Wniosek o konsultację	Komisja Europejska, 21.4.2021
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Jednolitego Rynku, Produkcji i Konsumpcji
Data przyjęcia przez sekcję	31.3.2021
Data przyjęcia na sesji plenarnej	27.4.2021
Sesja plenarna nr	560
Wynik głosowania	
(za/przeciw/wstrzymało się)	238/0/3

1. **Wnioski i zalecenia**

1.1. Europejski Komitet Ekonomiczno-Społeczny (EKES) uważa, że proponowana strategia jest pozytywnym krokiem w kierunku ochrony rządów, obywateli i przedsiębiorstw w całej UE przed globalnymi cyberzagrożeniami, a także w kierunku zabezpieczenia wzrostu gospodarczego.

1.2. EKES jest zdania, że należy udostępnić dodatkowe środki finansowania podmiotom państwowym, aby umożliwić inwestycje w infrastrukturę cyberbezpieczeństwa w celu skutecznej reakcję na kryzys, taki jak pandemia.

1.3. EKES z zadowoleniem przyjmuje propozycje utworzenia sieci ośrodków monitorowania bezpieczeństwa w całej UE oraz propozycję, by Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) współpracowała ze wszystkimi zainteresowanymi stronami w celu ograniczenia ryzyka stwarzanego przez sieć 5G.

1.4. EKES z zadowoleniem przyjmuje również propozycję dalszego rozwijania roli Europolu jako ośrodka wiedzy specjalistycznej na temat cyberprzestępczości. Za istotną uznaje również współpracę ze społecznością obejmującą wiele zainteresowanych stron, a także na szczeblu międzynarodowym.

1.5. EKES ostrzega przed niedoborem umiejętności w dziedzinie cyberbezpieczeństwa i zaleca korzystanie z ogólnounijnego narzędzia wytyczania ścieżek kariery w zakresie cyberbezpieczeństwa, które pomaga poszczególnym osobom w określaniu i budowaniu odpowiedniej ścieżki kariery i zarządzaniu nią.

1.6. EKES zwraca uwagę na kwestię dezinformacji. Rozpowszechnianie dezinformacji może mieć poważne konsekwencje, a zapobieganie jej powinno być częścią każdej strategii dotyczącej cyberbezpieczeństwa.

1.7. EKES zaleca, by wszelkie inwestycje zagraniczne w sektorach strategicznych w Unii były zgodne z polityką bezpieczeństwa UE.

1.8. EKES ostrzega przed pojawieniem się komputerów kwantowych i przed związanymi z tym zagrożeniami. Stąd istnieje potrzeba przejścia na kryptografię postkwantową – odporną na ataki komputera kwantowego.

1.9. EKES zaleca, by strategia Komisji w zakresie cyberbezpieczeństwa była regularnie aktualizowana, ale nie rzadziej niż co dwa lata, w celu skutecznego reagowania na przyszłe technologie i zagrożenia.

1.10. Wreszcie EKES podkreśla znaczenie dialogu społecznego w kształtowaniu polityki w zakresie cyberbezpieczeństwa, która skutecznie chroniłaby jednostki w trakcie telepracy i ogólnie działań on-line.

2. **Komunikat Komisji Europejskiej**

2.1. Celem komunikatu jest podkreślenie zaangażowania UE w ochronę środowiska internetowego, które zapewnia jak największą wolność i bezpieczeństwo z korzyścią dla jej obywateli.

2.2. W komunikacie przedstawiono wizję UE w tej dziedzinie, określono role i obowiązki, oraz zaproponowano konkretne działania na szczeblu UE mające na celu zapewnienie solidnej i skutecznej ochrony, przy jednoczesnej ochronie praw obywateli, tak aby zapewnić bezpieczne i chronione środowisko online.

2.3. Proponowane działania mają na celu:

— osiągnięcie cyberodporności poprzez zwiększenie zdolności, gotowości, współpracy, wymiany informacji i świadomości w dziedzinie bezpieczeństwa sieci i informacji w sektorze publicznym i prywatnym oraz na szczeblu krajowym i unijnym,

— standaryzację sekwencji procesów na potrzeby cyberobrony w całej Unii, a także stworzenie bazy danych zawierającej istotne informacje w celu zapewnienia danych analitycznych dotyczących zagrożeń z myślą o wsparciu dotkniętego sektora lub gospodarki,

— radykalne ograniczenie cyberprzestępczości poprzez zwiększenie wiedzy fachowej osób odpowiedzialnych za prowadzenie dochodzeń w sprawie cyberprzestępczości i jej ściganie, przyjęcie bardziej skoordynowanego podejścia między organami ścigania w całej Unii oraz zacieśnienie współpracy z innymi podmiotami,

— ustanowienie ogólnounijnego systemu edukacji i certyfikacji dla specjalistów, którzy spełniają wymogi dotyczące wykwalifikowanych ekspertów ds. cyberprzestępczości, i przekształcenie go w spójny ogólnounijny poziom umiejętności,

— opracowanie polityki i zdolności UE w zakresie cyberobrony w ramach wspólnej polityki bezpieczeństwa i obrony,

— wspieranie zasobów przemysłowych i technologicznych niezbędnych do korzystania z jednolitego rynku cyfrowego; będzie to bodźcem do powstania europejskiego przemysłu i rynku bezpiecznych technologii informacyjno-komunikacyjnych; przyczyni się do wzrostu gospodarczego i konkurencyjności gospodarki UE, a także zwiększy publiczne i prywatne wydatki na badania i rozwój w dziedzinie cyberbezpieczeństwa,

— wzmocnienie międzynarodowej polityki UE dotyczącej cyberprzestrzeni w celu promowania podstawowych wartości UE, określenia norm odpowiedzialnego zachowania, propagowania stosowania obowiązującego prawa międzynarodowego w cyberprzestrzeni oraz wspierania krajów spoza UE w budowaniu zdolności w zakresie cyberbezpieczeństwa,

— opracowanie i wdrożenie unijnej pieczęci bezpieczeństwa zatwierdzającej produkty, usługi i technologie spełniające normy i wymogi dotyczące rozwiązań cyberodpornych.

2.4. Proponowana strategia obejmuje bezpieczeństwo usług podstawowych, takich jak szpitale, sieci energetyczne i koleje, a także coraz większą liczbę podłączonych do sieci obiektów w naszych domach, biurach i fabrykach, budowanie wspólnych zdolności reagowania na znaczące cyberataki oraz współpracę z partnerami na całym świecie w celu zapewnienia międzynarodowego bezpieczeństwa i stabilności w cyberprzestrzeni.

2.5. Ponieważ zagrożenie dla cyberbezpieczeństwa niemal zawsze mają charakter transgraniczny, a cyberatak w jednym państwie może mieć wpływ na grupę państw członkowskich lub całą UE, Komisja proponuje ponadto utworzenie wspólnej jednostki ds. cyberprzestrzeni, aby jak najskuteczniej reagować na zagrożenia dla cyberbezpieczeństwa, wykorzystując wspólne zasoby i wiedzę fachową, którymi dysponują UE i państwa członkowskie.

2.6. Przedmiotowa strategia o wartości 2 mld EUR zostanie sfinansowana w ramach unijnych programów „Cyfrowa Europa" i „Horyzont Europa", z uwzględnieniem dodatkowych inwestycji ze strony państw członkowskich i sektora prywatnego.

3. **Uwagi ogólne**

3.1. Obecnie cyberbezpieczeństwo jest powszechnie akceptowane jako integralna część funkcjonowania instytucji i agencji UE oraz każdego państwa członkowskiego i jego gospodarki. Cyberbezpieczeństwo ma kluczowe znaczenie dla wspierania unijnej infrastruktury energetycznej i wdrażania inteligentnych sieci ([1]), a także cyfryzacji i ekologizacji gospodarek UE. Równie ważna jest ochrona i zabezpieczanie podstawowych praw i wolności obywateli, które gwarantuje cyberbezpieczeństwo. Ochrona praw i wolności ma szczególne znaczenie, ponieważ cyberataki mogą mieć negatywny wpływ na obywateli i gospodarstwa domowe (a także na przedsiębiorstwa, organizacje i służby publiczne). Niedawny atak komputerowy w ośrodku szpitalnym w Tournai w Belgii jest przykładem zagrożenia nie tylko dla dóbr materialnych, ale również dla życia ludzkiego ze względu na związane z nim opóźnienie operacji chirurgicznych ([2]).

3.2. Według DIGITALEUROPE ([3]) cyberzagrożenia stanowią istotną przeszkodę na drodze do osiągnięcia dobrobytu w Europie. Szacuje się, że do końca 2020 r. straty gospodarcze wynikające z cyberprzestępczości na całym świecie sięgną 2,5 bln EUR, a 74 % światowych przedsiębiorstw może spodziewać się ataku hakerskiego w 2021 r. Mimo tego tylko 32 % europejskich przedsiębiorstw prowadzi politykę w zakresie cyberbezpieczeństwa. Oczywiste jest, że zagrożenia cybernetyczne w sposób nieuchronny wymagają skoordynowanej reakcji ze strony UE i strategii w zakresie cyberbezpieczeństwa, zdolnej zarówno sprostać obecnym wyzwaniom, jak i bronić organizacji i obywateli przed cyberzagrożeniami następnej generacji. Dotyczy to w szczególności usług publicznych, w ramach których zarządza się ogromną ilością wrażliwych i osobowych danych wymagających ochrony. Ponadto należy zintensyfikować działania na rzecz osiągnięcia europejskiej suwerenności danych i zachowania poufności danych w Unii poprzez cyberodporność i odporność cyfrową, co z kolei zwiększy dobrobyt w UE.

3.3. Potencjalne straty gospodarcze wynikające z cyberataków są ogromne i obejmują:

— utratę własności intelektualnej i poufnych informacji handlowych,

— oszustwa internetowe i przestępstwa finansowe, często będące wynikiem kradzieży danych identyfikacyjnych,

— manipulację finansową, wykorzystywanie skradzionych szczególnie chronionych informacji handlowych dotyczących potencjalnych połączeń lub też wykorzystywanie wcześniejszej wiedzy na temat sprawozdań z wyników działalności notowanych na giełdzie spółek,

— koszty alternatywne, w tym zakłócenia w produkcji lub usługach, oraz zmniejszone zaufanie do działalności online,

— koszty zabezpieczenia sieci, takie jak zakup cyberubezpieczenia ([4]), oraz pokrycie kosztów związanych z przywracaniem stanu sprzed wystąpienia cyberataków,

— nadszarpnięcie reputacji i ryzyko odpowiedzialności cywilnej w przypadku zhakowanego przedsiębiorstwa i jego marki, w tym tymczasowy spadek wartości akcji.

3.4. Warto zauważyć, że skutki gospodarcze cyberprzestępczości są największe w Europie i według szacunków plasują się na poziomie 0,84 % PKB UE w porównaniu z 0,78 % w Ameryce Północnej – jak wynika z najnowszego sprawozdania na temat gospodarczych skutków cyberprzestępczości, sporządzonego przez Centrum Studiów Strategicznych i Międzynarodowych (CSIS).

3.5. W tym kontekście proponowana strategia, opracowana w drodze szeroko zakrojonych konsultacji z zainteresowanymi stronami, pojawiła się w najlepszym możliwym momencie, a eksperci przewidują, że do 2025 r. liczba urządzeń podłączonych do sieci na całym świecie wzrośnie do 25 mld. Oczekuje się, że jedna czwarta tych urządzeń będzie znajdować się w Europie.

([1]) Cyberataki na inteligentną sieć mogłyby wpłynąć na dostawy energii dla konsumentów i przedsiębiorstw.
([2]) https://www.databreaches.net/chwapi-hospital-hit-by-ransomware-operations-canceled-and-another-city-hit/
([3]) https://www.digitaleurope.org/
([4]) Usługi cyberubezpieczenia nie są oczywiście dostępne w nieograniczonym zakresie. W rzeczy samej COVID-19 uwypuklił fakt, że nagromadzenie ryzyka stanowi wyzwanie dla ubezpieczenia. Niedawne badania przeprowadzone przez firmę AON potwierdzają, że ubezpieczenie stanowi jedynie bardzo niewielką (5 %) część wydatków na cybergotowość. Okazało się, że audyty i szkolenia są ważniejszymi czynnikami wpływającymi na koszty.

3.6. Zapowiedź strategii zbiegła się z doniesieniami o zainfekowaniu komputerów w amerykańskich federalnych agencjach rządowych w wyniku cyberataku wymierzonego w firmę z USA opracowującą oprogramowanie dla firm pomagające im zarządzać ich sieciami i systemami IT. Setki amerykańskich korporacji również były narażone na ten atak, w trakcie którego hakerzy dodawali złośliwe oprogramowanie do aktualizacji oprogramowania, którą pobrało tysiące klientów firmy będącej celem ataku. Incydent ten pokazuje, że administracje publiczne i przedsiębiorstwa we wszystkich sektorach i całe społeczeństwo mogą być narażone na cyberataki.

3.7. Nie dziwi więc, że omawiana strategia obejmuje kluczowe sektory, w tym dostawców danych i usług w chmurze, telekomunikację, rządowe systemy informatyczne i produkcję. Inne istotne przykłady potencjalnych zagrożeń dla cyberbezpieczeństwa obejmują aplikacje służące ustalaniu kontaktów zakaźnych, takie jak te stosowane w odpowiedzi na COVID-19. Zabezpieczenie aplikacji służących ustalaniu kontaktów zakaźnych w oczywisty sposób przyczynia się do zwiększenia zaufania obywateli do ochrony danych prywatnych w odniesieniu do środków związanych z COVID-19, które uznano za niezbędne w reakcji na pandemię.

3.8. Pandemia COVID-19 przyspieszyła zmianę modeli pracy: w 2020 r. aż 40 % pracowników w UE przestawiło się na telepracę ([5]). Szacuje się jednak, że w 2020 r. 40 % użytkowników w UE doświadczyło problemów związanych z bezpieczeństwem, przy czym ponad 12 % przedsiębiorstw zostało dotkniętych cyberatakami.

4. **Uwagi szczegółowe**

4.1. EKES uważa, że proponowana strategia stanowi krok we właściwym kierunku, by chronić rządy, obywateli i przedsiębiorstwa w całej UE przed globalnymi cyberzagrożeniami i zapewnić przywództwo w cyberprzestrzeni, przy jednoczesnym zapewnieniu wszystkim możliwości czerpania korzyści z internetu i ze stosowania technologii.

4.2. EKES jest zdania, że cyberbezpieczeństwo ma kapitalne znaczenie dla ochrony działalności gospodarczej i pobudzania wzrostu gospodarczego, a także dla zapewnienia zaufania użytkowników do działalności w internecie. Podziela również pogląd, że potrzebne są odważne działania, aby zapewnić Europejczykom możliwość bezpiecznego korzystania z innowacji, łączności i automatyzacji.

4.3. EKES dostrzega, że sektory gospodarki UE stają się coraz bardziej zależne od technologii cyfrowych, a także od siebie nawzajem. Nastąpił również ogromny wzrost wykorzystania urządzeń internetu rzeczy (IoT) przez konsumentów i przedsiębiorstwa, a także w środowiskach przemysłowych, takich jak produkcja, podczas gdy technologie finansowe i regulacyjne również przenikają do głównego nurtu. Rozwój sieci 5G nabrał tempa, a ostatnio kryzys związany z COVID-19 przyspieszył transformację cyfrową wielu przedsiębiorstw i rządów, zmuszając je do prowadzenia działalności zdalnie niemal z dnia na dzień, przy znacznym wykorzystaniu usług opartych na chmurze obliczeniowej. Tego rodzaju zmiany wymagają skutecznej, szybkiej i inkluzywnej reakcji w zakresie cyberbezpieczeństwa.

4.4. Zmiany te zwiększyły poziom ryzyka krytycznego, na który narażone są rządy i przemysł. W związku z tym EKES popiera nową strategię w zakresie cyberbezpieczeństwa i jej szereg propozycji mających na celu poprawę cyberodporności zarówno w UE, jak i poza nią. Chociaż podmioty publiczne kwalifikują się do finansowania unijnego w ramach różnych odpowiednich programów wspierających inwestycje w tej dziedzinie, takich jak „Horyzont 2020”/„Horyzont Europa”, EKES uważa, że być może należałoby stworzyć dalsze możliwości finansowania dla podmiotów publicznych lub mających częściowo publiczny charakter, aby umożliwić inwestycje na rzecz odpowiedniej infrastruktury cyberbezpieczeństwa, aby zapewnić bezpieczeństwo dostaw dla obywateli, zwłaszcza w czasach kryzysu, takiego jak pandemia.

4.5. Propozycja Komisji Europejskiej dotycząca utworzenia sieci ośrodków monitorowania bezpieczeństwa w całej UE, w ramach których wykorzystywano by sztuczną inteligencję i uczenie maszynowe w celu poprawy wykrywania zagrożeń i incydentów, a także ich analizy i szybkości reagowania, jest ważna i została zgłoszona we właściwym momencie. EKES przyznaje, że ręczne zapobieganie udanym cyberatakom staje się coraz trudniejsze ze względu na to, że zespoły ds. bezpieczeństwa muszą zajmować się ogromną liczbą codziennych alarmów, a także z powodu ogólnego niedoboru wyspecjalizowanych pracowników w tej dziedzinie. Wszystko to sprawia, że automatyzacja ośrodków monitorowania bezpieczeństwa jest nieunikniona.

([5]) Eurofound (2020), *Living, working and COVID-19*, seria „COVID-19”, Urząd Publikacji Unii Europejskiej, Luksemburg.

4.6. EKES z zadowoleniem przyjmuje cele i działania w zakresie bezpieczeństwa sieci 5G, które będą miały kapitalne znaczenie dla ograniczenia nowych zagrożeń wynikających z rosnącej powierzchni ataku, którą stworzy infrastruktura sieci 5G. Zwłaszcza zaś popiera apel do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i państw członkowskich o współpracę ze wszystkimi zainteresowanymi stronami w celu lepszego zrozumienia nowych technologii i zdolności w zakresie bezpieczeństwa sieci 5G oraz związanych z tym zagrożeń. Jasne jest, że uznano w strategii, iż nowe technologie wykorzystywane przez sieci 5G – takie jak wirtualizacja sieci, warstwowanie sieci i przetwarzanie danych na obrzeżach sieci – są szczególnie narażone na konkretne podatności, co sprawia, że wymagają one dodatkowych środków bezpieczeństwa.

4.7. EKES z zadowoleniem przyjmuje propozycję dalszego zwiększania roli Europolu jako ośrodka wiedzy fachowej na temat cyberprzestępczości w celu wspierania krajowych organów ścigania, a także zwiększenia finansowania i wzmocnienia mandatu CERT-UE. Oba podmioty odgrywają kluczową rolę we wspieraniu działań na rzecz cyberbezpieczeństwa w całej UE. Wysiłki te niewątpliwie przyczynią się do poprawy cyberbezpieczeństwa instytucji i agencji UE oraz innych podmiotów.

4.8. EKES z zadowoleniem przyjmuje fakt, że w strategii położono nacisk na współpracę międzynarodową UE, np. poprzez dyplomację cyfrową w stosunkach międzynarodowych, zintensyfikowanie dwustronnych dialogów na temat cyberbezpieczeństwa i budowanie zdolności cyfrowych w państwach trzecich. Zagrożenia dla cyberbezpieczeństwa mają charakter globalny, a nie tylko regionalny, zatem skuteczna polityka przeciwdziałania im także musi mieć charakter globalny.

4.9. EKES odnotowuje, że w strategii podkreślono znaczenie dialogu i współpracy w społeczności obejmującej wiele zainteresowanych stron, zwłaszcza poprzez regularną wymianę informacji z sektorem prywatnym i publicznym, partnerami społecznymi i środowiskiem akademickim. Podejście to jest pożądane i będzie miało zasadnicze znaczenie dla dalszego uszczegółowienia propozycji zawartych w strategii oraz zajęcia się ważnymi nowymi sprawami, takimi jak wyzwania w zakresie bezpieczeństwa związane z telepracą. Wszystkie zainteresowane strony powinny stale wnosić wkład w ten proces, ponieważ poziom technologii wykorzystywanej w cyberprzestępczości staje się bardziej wyrafinowany.

4.10. EKES z zadowoleniem przyjmuje położenie nacisku na rozwój odpowiednich umiejętności ogólnie chroniących przed cyberzagrożeniami. Jednak w przypadku większości europejskich przedsiębiorstw, a zwłaszcza MŚP, rosnąca luka kompetencyjna pozostaje ogromnym problemem w walce z zagrożeniami w zakresie cyberbezpieczeństwa. EKES uważa, że temu brakowi kwalifikacji można zaradzić jedynie za pomocą ogólnounijnego narzędzia wytyczania ścieżek kariery w zakresie cyberbezpieczeństwa, które pomaga poszczególnym osobom w określaniu i budowaniu odpowiedniej ścieżki kariery i zarządzaniu nią dzięki lepszemu zrozumieniu wiedzy, umiejętności i zdolności potrzebnych do rozpoczęcia i rozwoju kariery w dziedzinie cyberbezpieczeństwa lub przekwalifikowania się w tej dziedzinie. Narzędzie to powinno również obejmować konkretne programy dotyczące dostępności i różnorodności w przestrzeni cyberbezpieczeństwa. Uznaje się kluczową rolę instytucji kształcenia i szkolenia zawodowego (VET) we wspieraniu ogólnounijnego narzędzia wytaczania ścieżek kariery w zakresie cyberbezpieczeństwa. Ponadto UE powinna w coraz większym stopniu dążyć do wspólnych inicjatyw badawczych (w UE i poza nią) w celu kształcenia wykwalifikowanych specjalistów z odpowiednimi umiejętnościami w dziedzinie cyberbezpieczeństwa w sposób sprzyjający włączeniu społecznemu, zważywszy na ewoluującą rolę technologii w tworzeniu bardziej integracyjnego miejsca pracy i społeczeństwa. Ponadto należy intensywnie rozważyć zachęcanie studentek i studentów do podejmowania studiów wyższych w dziedzinie cyberbezpieczeństwa poprzez przyznawanie stypendiów na studia licencjackie, magisterskie i studia drugiego lub trzeciego stopnia koncentrujące się na cyberbezpieczeństwie, w zamian za pracę na rzecz instytucji i agencji UE, a także organów publicznych w całej UE po ukończeniu studiów.

4.11. EKES zauważa, że związek między cyberbezpieczeństwem a dezinformacją jest aspektem, który nie został uwzględniony w strategii w zakresie cyberbezpieczeństwa. W ujęciu konkretnym EKES pragnie odnieść się do badania zleconego przez Departament Tematyczny ds. Praw Obywatelskich i Spraw Konstytucyjnych Parlamentu Europejskiego ([6]). W epoce cyberprzestrzeni internetowej rozpowszechnianie dezinformacji może mieć poważne konsekwencje. Ataki transgraniczne mogą być ukierunkowane na ośrodki informacyjne, instytucje rządowe lub europejskie w celu rozpowszechniania dezinformacji, a tego rodzaju ataki mogą również zmniejszyć zaufanie do organów publicznych. W związku z tym w każdej strategii w zakresie cyberbezpieczeństwa należy położyć nacisk na zapobieganie dezinformacji.

4.12. EEKS odnotowuje ponadto, że inwestycje zagraniczne w sektorach strategicznych, nabywanie krytycznych aktywów i technologii, a także infrastruktury krytycznej w Unii oraz dostawy urządzeń mających krytyczne znaczenie również mogą stanowić zagrożenie dla bezpieczeństwa Unii. W związku z tym, zgodnie z obowiązującymi przepisami dotyczącymi zamówień publicznych EKES zaleca, by przy udzielaniu zamówień przywiązywano większą wagę do kwestii bezpieczeństwa.

([6]) http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

4.13. EKES odnotowuje, że bezpieczeństwo obecnego oprogramowania kryptograficznego i systemów kryptograficznych jest zagrożone przez pojawienie się komputerów kwantowych, które mają być publicznie dostępne w ciągu dziesięciu lat lub jeszcze szybciej. Stąd potrzeba przejścia na kryptografię odporną na komputery kwantowe – kryptografię postkwantową. Świadczą o tym światowe inicjatywy na rzecz standaryzacji postkwantowych systemów kryptograficznych, takie jak amerykański proces normalizacji kryptografii postkwantowej NIST, utworzenie grupy roboczej ds. kryptografii kwantowej w ramach Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI) oraz konkurs poświęcony kryptografii postkwantowej organizowany przez Chińskie Stowarzyszenie na rzecz Badań Kryptograficznych.

4.14. EKES zaleca dokonanie przeglądu krajowych strategii w zakresie cyberbezpieczeństwa w celu zapewnienia spójności ze strategią Komisji i zbieżności decyzji podejmowanych na szczeblu państw członkowskich z propozycjami zawartymi w strategii Komisji. Ogólnounijna strategia oraz strategie krajowe powinny być zbieżne, aby skutecznie radzić sobie z cyberzagrożeniami – zarówno obecnie, jak i w przyszłości.

4.15. Z uwagi na to, że przyszłe zagrożenia są w znacznym stopniu nieprzewidywalne, i w nawiązaniu do pkt 4.13 powyżej EKES zaleca, by strategia Komisji w zakresie cyberbezpieczeństwa była regularnie aktualizowana przynajmniej co dwa lata w celu skutecznego reagowania na przyszłe technologie i zagrożenia. Jak stwierdzono wcześniej, zaangażowanie zainteresowanych stron i badania prowadzone na wysokim szczeblu będą również miały kluczowe znaczenie dla aktualizacji strategii w zakresie cyberbezpieczeństwa.

Bruksela, dnia 27 kwietnia 2021 r.

Christa SCHWENG
Przewodnicząca
Europejskiego Komitetu Ekonomiczno-Społecznego