Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wspólny komunikat do Parlamentu Europejskiego i Rady »Polityka UE w zakresie cyberobrony«”

(opinia z inicjatywy własnej)

(2023/C 293/04)

Sprawozdawca: **Anastasis YIAPANIS**

Współsprawozdawca: **Alberto MAZZOLA**

Decyzja Zgromadzenia Plenarnego	20.9.2022
Podstawa prawna	Art. 52 ust. 2 regulaminu wewnętrznego
	Opinia z inicjatywy własnej
Sekcja odpowiedzialna	Komisja Konsultacyjna ds. Przemian w Przemyśle (CCMI)
Data przyjęcia przez sekcję	27.3.2023
Data przyjęcia na sesji plenarnej	14.6.2023
Sesja plenarna nr	579
Wynik głosowania	
(za/przeciw/wstrzymało się)	208/1/2

1. **Wnioski i zalecenia**

1.1. Europejski Komitet Ekonomiczno-Społeczny (EKES) popiera proponowaną politykę UE w zakresie cyberobrony, lecz spodziewał się, że zorganizowane społeczeństwo obywatelskie odegra bardziej znaczącą rolę w opracowywaniu tych propozycji. Na obecnym etapie trudno jest mu ocenić, czy przyszłe inicjatywy przedstawione we wspólnym komunikacie zostaną zrealizowane i przyniosą zamierzone efekty. EKES wzywa instytucje UE i państwa członkowskie do priorytetowego potraktowania zapowiedzianych inicjatyw i ich szybkiego podjęcia.

1.2. Komitet podkreśla potrzebę wprowadzenia dodatkowych środków w celu zwiększenia zdolności UE do wykrywania zagrożeń cyberbezpieczeństwa i apeluje o przeznaczenie środków finansowych na badania i rozwój, aby umożliwić postępy w zakresie najnowocześniejszych zdolności UE. Współpraca między sektorem prywatnym i publicznym ma zasadnicze znaczenie i nie może być jednokierunkowa. EKES uważa, że koordynacja na szczeblu UE jest konieczna, aby rozwiązać problem fragmentacji i zapewnić współpracę oraz możliwość realizowania wspólnych inwestycji między państwami członkowskimi.

1.3. EKES popiera utworzenie Centrum Koordynacji UE ds. Cyberobrony i zaleca, aby państwa członkowskie zobowiązały się do całodobowego szybkiego reagowania, oceny gotowości cybernetycznej i skuteczności unijnych mechanizmów reagowania na cyberkryzysy, ze szczególnym uwzględnieniem zarówno zdolności wojskowych, jak i sektorów krytycznych określonych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555 (dyrektywa NIS 2) ([1]). Popiera rozszerzenie mandatu Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) w celu wspierania prac Centrum Koordynacji UE ds. Cyberobrony.

1.4. EKES opowiada się za opracowaniem lub przejęciem od sektora prywatnego dynamicznej platformy testowania i wymiany informacji w czasie rzeczywistym w celu wzmocnienia strategicznej autonomii i suwerenności Unii w zakresie cyberbezpieczeństwa oraz w celu wykrycia istniejących luk w obecnych zdolnościach. Platformę można również wykorzystać do wymiany najlepszych praktyk, zgłaszania cyberincydentów oraz do stworzenia unijnego wykazu wszystkich cyberprzestępców.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

1.5. Komitet podkreśla potrzebę lepszego przygotowania się na cyberataki, takie jak ataki rosyjskie na Ukrainę ukierunkowane w szczególności na infrastrukturę krytyczną. Współpraca między ekosystemami cywilnym i wojskowym ma kluczowe znaczenie dla skutecznego zarządzania kryzysowego, interoperacyjności i unikania powielania wysiłków i inwestycji, w tym przez symulowane testowe cyberataki.

1.6. EKES uważa, że w inwestycjach w cyberobronę należy postawić na pierwszym miejscu ochronę obywatelek i obywateli UE i infrastruktury krytycznej, między innymi polegając na zaufanych dostawcach sprzętu i oprogramowania. Podkreśla potrzebę terminowego aktualizowania priorytetów i inwestycji, które mają zostać uzgodnione przez UE i państwa członkowskie, z udziałem odpowiednich zainteresowanych stron z sektora prywatnego.

1.7. UE musi zachować i rozwijać zdolności niezbędne do zabezpieczenia swoich: gospodarki cyfrowej, społeczeństwa, demokracji i technologii krytycznych oraz do świadczenia kluczowych usług w zakresie cyberbezpieczeństwa. Zasadnicze znaczenie dla zapewnienia strategicznej autonomii UE ma zmniejszenie zależności od państw trzecich. EKES uważa, że konieczne jest, aby UE przyjęła oparte o perspektywę średnioterminową podejście do autonomii w odniesieniu do kluczowych technologii, i zdecydowanie opowiada się za utworzeniem obiektów badawczych i produkcyjnych przez przedsiębiorstwa z siedzibą w UE, przy czym odpowiednia europejska polityka przemysłowa skupiałaby się na autonomicznym ekosystemie cyberbezpieczeństwa.

1.8. MŚP powinny otrzymywać ukierunkowane wsparcie i mieć dostęp do programów finansowania, które zwiększają ich odporność na cyberataki, a także do pomocy oraz możliwości szkolenia i kształcenia w zakresie ryzyka w cyberprzestrzeni i sposobów ochrony przed tym ryzykiem. UE powinna zapewnić mechanizm zachęt sprzyjający stopniowemu zaznajamianiu się MŚP z tą wiedzą oraz rozwojowi innowacyjnych MŚP.

1.9. EKES popiera plan utworzenia Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa i zwraca się do Komisji Europejskiej, aby koordynowała i finansowała zakrojone na szeroką skalę programy szkoleń i kształcenia zawodowego z udziałem wszystkich państw członkowskich, mające na celu wykształcenie wykwalifikowanej siły roboczej dla wszystkich agencji i organizacji zaangażowanych w cyberobronę, a także dla prywatnych sieci cywilnych.

1.10. Komitet uważa, że podnoszenie świadomości obywateli na temat cyberbezpieczeństwa ma zasadnicze znaczenie dla ograniczenia narażenia na cyberataki, i apeluje o opracowywanie programów nauczania w zakresie cyberbezpieczeństwa i programów szkoleń przez całe życie, które skupią się na poprawie umiejętności i wiedzy w dziedzinie cyberbezpieczeństwa. Popiera uwzględnianie aspektu cyberbezpieczeństwa we wszystkich przyszłych politykach publicznych UE oraz informowanie ogółu społeczeństwa o zagrożeniach cyberbezpieczeństwa.

1.11. EKES uważa, że ścisła współpraca z sojusznikami NATO w obszarach wojskowych musi koncentrować się na pełnej koordynacji i wzajemności, wspólnych projektach w zakresie badań, rozwoju i innowacji, wymianie najlepszych praktyk, szeroko zakrojonych programach szkoleniowych i symulacji cyberataków, których głównym celem jest zwiększenie wspólnej zdolności reagowania.

1.12. Komitet wzywa wysokiego przedstawiciela do przeanalizowania obecnych dwustronnych dialogów w sprawach cyberprzestrzeni i do zaangażowania się w dodatkowe dyskusje z innymi państwami i odpowiednimi organizacjami międzynarodowymi w celu ustanowienia ogólnoświatowych ram przestrzegania prawa międzynarodowego w cyberprzestrzeni, ze szczególnym naciskiem na wzajemność. Sądzi, że UE jest dobrze przygotowana do objęcia przewodnictwa w międzynarodowych dyskusjach na temat przyszłości cyberbezpieczeństwa, zwłaszcza w ramach Organizacji Narodów Zjednoczonych, ponieważ stworzyła solidne podwaliny w postaci podstawowych swobód demokratycznych.

1.13. UE powinna stanowczo sprzeciwiać się wszelkiego rodzaju systemom scoringu obywateli. EKES jasno stwierdza, że prawdziwa demokracja nie może istnieć bez efektywnej ochrony danych osobowych, a także uważa, że odpowiedzialne i skuteczne zarządzanie danymi ma kapitalne znaczenie dla przekształcenia hiperłączności w przewagę konkurencyjną.

2. **Wprowadzenie i uwagi ogólne**

2.1. Rozwój cyfrowy społeczeństw wiąże się z dużą liczbą zagrożeń cyberbezpieczeństwa spowodowanych modernizacją technologiczną. W ciągu ostatnich kilku lat liczba cyberataków znacznie wzrosła, a ponadto wyraźnie podniósł się poziom ich zaawansowania, co stanowi zagrożenie dla bezpieczeństwa zarówno podmiotów publicznych, jak i prywatnych. Niezależnie od tego, czy chodzi o oprogramowanie szantażujące, złośliwe oprogramowanie, ataki za pośrednictwem poczty elektronicznej, naruszenia ochrony danych, dezinformację, rozproszone ataki typu „odmowa usługi" lub inne formy ataków, wszystkie one stanowią stałe i ciągłe zagrożenie dla bezpieczeństwa całej UE.

2.2. EKES z zadowoleniem przyjmuje wspólny komunikat w sprawie *polityki UE w zakresie cyberobrony* ([2]) i uważa, że nadszedł czas, aby podjąć działania w trybie pilnym i skoordynowanym na szczeblu UE, obejmujące zarówno cywilny, jak i wojskowy ekosystem cyberprzestrzeni oraz zapewniające odpowiednie ramy inwestycyjne dla zdolności cyberobronnych. Zauważa jednak, że komunikat jest jedynie deklaracją determinacji do działania i wykazem przyszłych inicjatyw UE, które powinny zostać zrealizowane, i uważa, że nie można ocenić, czy te przyszłe zobowiązania zostaną faktycznie podjęte, ponieważ przyszłe negocjacje między współprawodawcami w naturalny sposób wpłyną na ostateczny wynik unijnego planu działania w zakresie cyberbezpieczeństwa.

2.3. Rosyjski atak na sieć satelitarną KA-SAT, który zakłócił komunikację między ukraińskimi siłami wojskowymi, oraz niedawny skandal z udziałem Érica Léandriego, któremu część przedsiębiorstw działających w branży obronności zleciła cyberszpiegostwo w ich imieniu, stawiają cyberbezpieczeństwo na czele listy zagrożeń bezpieczeństwa w UE. Chociaż RODO jest solidnym aktem prawnym UE i obowiązuje od kilku lat, oczywiste jest, że coraz większa ilość dostępnych danych jest podatna na zagrożenia, a ryzyko przekroczenia przez osoby trzecie granicy legalności rośnie z każdym dniem.

2.4. Biorąc pod uwagę transgraniczny charakter cyberataków, konieczna jest koordynacja na szczeblu UE, aby zmniejszyć obecną fragmentację i zapewnić gotowość państw członkowskich do współpracy i wspólnego inwestowania. Jest to szczególnie istotne w odniesieniu do przyszłych scenariuszy takich ataków, w których jedno państwo członkowskie może być celem, a wszystkie inne powinny mieć możliwość udzielenia natychmiastowego wsparcia.

3. **Wspólne działania na rzecz silniejszej cyberobrony**

3.1. Komitet przyjmuje do wiadomości zapowiedziane ambitne inicjatywy na rzecz utworzenia Centrum Koordynacji UE ds. Cyberobrony, opracowania projektu CyDef-X, powołania zespołów szybkiego reagowania na cyberincydenty, opracowania inicjatywy na rzecz cybersolidarności UE oraz zbadania możliwości opracowania systemów certyfikacji cyberbezpieczeństwa produktów, usług i procesów ICT. Zaleca, aby wszystkie państwa członkowskie zobowiązały się do gotowości do zapewnienia szybkiego reagowania w systemie całodobowym, przy czym Centrum Koordynacji UE ds. Cyberobrony powinno brać udział w ocenie i opracowywaniu regularnych sprawozdań na temat gotowości cybernetycznej państw członkowskich oraz skuteczności europejskiego mechanizmu reagowania na cyberkryzysy, ze szczególnym uwzględnieniem zarówno zdolności wojskowych, jak i sektorów krytycznych określonych w dyrektywie NIS 2. Każde państwo członkowskie powinno dysponować specjalistami specjalnie przeszkolonymi do interweniowania w przypadku cyberincydentów oraz powinno regularnie sprawdzać ich zdolność interwencji w innych państwach członkowskich.

3.2. Choć w komunikacie przedstawiono długą listę wprowadzanych stopniowo udoskonaleń, to EKES opowiada się za tym, aby określono wyraźny plan działania dotyczący realizacji tych inicjatyw, z doprecyzowanymi mechanizmami zarządzania i wyznaczonymi terminami składania i przyjmowania wniosków. Ponadto Komitet oczekiwałby, że zorganizowane społeczeństwo obywatelskie odegra bardziej znaczącą rolę w opracowywaniu tych propozycji.

3.3. EKES uważa, że państwa członkowskie muszą zwiększyć swoje wewnętrzne zdolności w zakresie przeciwdziałania zagrożeniom cyberbezpieczeństwa, angażując się zarazem w projekty współpracy oraz dzieląc się informacjami i najlepszymi praktykami ze swoimi odpowiednikami w innych państwach członkowskich. Potrzebne są szybkie inwestycje w zdolności cyberobronne oraz we wspólną gotowość do wykrywania cyberataków, obrony przed nimi i do usuwania ich skutków, a także niezbędne jest przyspieszone wdrażanie technologii ([3]) we wszystkich państwach członkowskich. Komitet uważa, że aby wspierać autonomię Unii w zakresie cyberbezpieczeństwa, należy opracować lub przejąć od sektora prywatnego dynamiczną platformę testowania i wymiany informacji w czasie rzeczywistym, która będzie koncentrować się na wykrywaniu obecnie brakujących zdolności.

3.4. EKES podziela pogląd, że na tym etapie wojskowe operacje w cyberprzestrzeni powinny pozostać wyłącznie w gestii państw członkowskich; popiera zapowiadaną współpracę między unijnymi wojskowymi zespołami reagowania na incydenty komputerowe (milCERT), zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz zespołem reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE).

3.5. Niedawno przyjęta dyrektywa NIS 2 i dyrektywa w sprawie odporności podmiotów krytycznych (CER) ([4]) wprowadziły już szczegółowe obowiązki krajowe i sektorowe dotyczące unijnych ram cyberobrony. Konieczne są dalsze działania w celu poprawy wspólnych zdolności UE w zakresie wykrywania, a EKES apeluje o inwestowanie w badania i rozwój w celu rozwijania najnowocześniejszych zdolności UE.

([2]) Komunikat Komisji „Polityka UE w zakresie cyberobrony".
([3]) Takie jak inicjatywa NATO – Akcelerator Innowacji Obronnych dla Północnego Atlantyku (DIANA).
([4]) Dyrektywa CER.

4. **Zabezpieczenie ekosystemu obronnego UE**

4.1. EKES jest zdania, że nieodłączna złożoność i szybko zmieniające się wyzwania technologiczne zmieniły ekosystem obronny, a cyberbezpieczeństwo stało się wspólnym tematem zarówno dla sektora wojskowego, jak i cywilnego, a także dla obywateli UE. Współpraca między ekosystemami cywilnym i wojskowym jest obecnie ważniejsza niż kiedykolwiek i powinna przynieść korzyści pod względem skuteczniejszego zarządzania kryzysowego, a także stałego postępu i interoperacyjności, przy uniknięciu powielania lub mnożenia tych samych wysiłków i inwestycji. Państwa członkowskie powinny być gotowe do przeprowadzenia testów warunków skrajnych krajowej infrastruktury krytycznej w celu oceny i zwiększenia odporności na przyszłe cyberataki.

4.2. EKES jest zdania, że inwestycje w cyberobronę muszą być ukierunkowane przede wszystkim na ochronę obywateli UE i unijnej infrastruktury krytycznej. Biorąc pod uwagę szybkie tempo transformacji cyfrowej i błyskawicznie zmieniający się krajobraz zagrożeń, Komitet zdecydowanie wzywa UE i państwa członkowskie do uzgodnienia terminowych aktualizacji priorytetów i inwestycji po przeprowadzeniu szczegółowych konsultacji z odpowiednimi zainteresowanymi stronami z sektora prywatnego. Urządzenia internetu rzeczy (IoT) często nie są tak dobrze chronione jak urządzenia tradycyjne, dlatego EKES apeluje o zapewnienie minimalnego poziomu bezpieczeństwa za pośrednictwem platform zarządzania uprawnieniami i tożsamością użytkowników. Ponadto, ponieważ certyfikacja jest główną metodą zapewnienia wyższego poziomu bezpieczeństwa, Komitet apeluje o położenie większego nacisku na bezpieczeństwo internetu rzeczy w ramach nowego podejścia UE do certyfikacji.

4.3. UE musi budować odporność na cyberataki i tworzyć skuteczną cyberprewencję. Należy chronić infrastrukturę krytyczną przed wszelkiego rodzaju cyberatakami, w tym przez unijne systemy obronne. Komitet uważa, że w strategicznym interesie UE leży zapewnienie, aby Unia utrzymywała i rozwijała podstawowe zdolności do zabezpieczenia swoich: gospodarki cyfrowej, społeczeństwa i demokracji, osiągnięcia pełnej suwerenności cyfrowej jako jedynego sposobu ochrony technologii krytycznych i świadczenia skutecznych kluczowych usług w zakresie cyberbezpieczeństwa. Zmniejszenie zależności od państw trzecich ma również zasadnicze znaczenie dla strategicznej autonomii UE. EKES sądzi, że powinno się zaangażować w ten proces sektorowe agencje UE (ENISA, EASA, ERA, EMA, EUNB, ESA, HADEA itp.), które powinny zapewnić wytyczne przy opracowywaniu systemów cyberbezpieczeństwa.

4.4. Pandemia COVID-19 przyspieszyła transformację cyfrową i przekształciła pracę tradycyjną w hybrydową lub zdalną, co spowodowało powstanie nowych stosunków pracy i oczekiwań, a także nowej klasy cyfrowych nomadów, których liczba rośnie. EKES odnotowuje szybkie zmiany na rynku pracy, które doprowadziły do przyjęcia przez przedsiębiorstwa architektury zerowego zaufania za pośrednictwem takich rozwiązań, jak system zarządzania uprawnieniami i tożsamością użytkowników oraz zarządzanie uprzywilejowanym dostępem. Komitet uważa, że taki rodzaj zarządzania zasobami przedsiębiorstw zapewnia nowe rozwiązania w zakresie zagrożeń cyberbezpieczeństwa i że należy wspierać sektor prywatny w podnoszeniu poziomu bezpieczeństwa swoich innowacyjnych rozwiązań cyfrowych.

4.5. EKES wyraża raczej rozczarowanie stwierdzeniem Komisji, że „można rozważyć możliwość opracowania planu wdrażania we współpracy z państwami członkowskimi", i jest zdania, że taki plan wdrażania jest obowiązkowy. Uważa, że należy go opracować wspólnie z państwami członkowskimi i jak najszybciej wdrożyć. Komitet jest zaniepokojony łagodnym stanowiskiem Komisji i wzywa instytucje UE oraz państwa członkowskie do ułatwienia szybkich postępów w realizacji zapowiedzianych inicjatyw.

5. **Inwestowanie w zdolności cyberobronne**

5.1. Wraz z szybkim rozwojem technologicznym cyberprzestrzeń stała się najnowszym obszarem działań wojennych – po lądzie, morzu, powietrzu i przestrzeni kosmicznej. Stworzyło to również duże możliwości przestępczości dla działających w złej wierze podmiotów cybernetycznych, począwszy od niezależnych hakerów, a skończywszy na zawodowych przestępcach, a nawet na podmiotach państwowych.

5.2. Inwestycje w badania i rozwój mają zasadnicze znaczenie i EKES z zadowoleniem przyjmuje istniejące specjalne fundusze w ramach programu „Cyfrowa Europa", Europejskiego Funduszu Obronnego, programu „Horyzont Europa" i krajowych planów odbudowy i zwiększania odporności. Komitet życzyłby sobie jednak większej liczby projektów transnarodowych, które koncentrują się na współpracy i interoperacyjności systemów cyberobrony we wszystkich państwach członkowskich, a także większej synergii między instrumentami finansowania, zwłaszcza dla innowacyjnych MŚP.

5.3. Komitet zauważa, że – jak zapowiedziano w unijnej strategii cyberbezpieczeństwa w 2020 r. – termin utworzenia wspólnej jednostki ds. cyberprzestrzeni przypada w tym roku, i oczekuje informacji na temat zakończenia tego procesu i gotowości UE do reagowania na cyberincydenty na dużą skalę. Oczekuje, że poprawi to orientację sytuacyjną UE oraz jej ogólną zdolność reagowania i odbudowy.

5.4. EKES popiera rozszerzenie mandatu ECCC, tak by mogło wspomagać działalność Centrum Koordynacji UE ds. Cyberobrony. Ponadto ta sieć mogłaby wspierać europejską suwerenność cyfrową przez rozwój konkurencyjnej europejskiej bazy przemysłowej dla kluczowych zdolności technologicznych, częściowo w oparciu o prace prowadzone w ramach umownych partnerstw publiczno-prywatnych (PPP). PPP okazały się najskuteczniejszym podejściem umożliwiającym poprawę cyberbezpieczeństwa całego ekosystemu cyfrowego, ale ich działanie nie może być jednokierunkowe – instytucje publiczne muszą również dzielić się swoimi informacjami z sektorem prywatnym.

5.5. EKES zauważa, że aby zaradzić przyszłym próbom hakowania z użyciem komputerów kwantowych, UE musi natychmiast zainwestować w najnowocześniejsze technologie, takie jak kryptografia postkwantowa. Uważa, że konieczne jest, aby Europa przyjęła oparte o perspektywę średnioterminową podejście do autonomii, i zdecydowanie opowiada się za rozwojem zakładów badawczych i produkcyjnych przez przedsiębiorstwa z siedzibą w UE. EKES jest zdania, że ważne jest zwiększenie zasobów UE na cyfrowe badania naukowe i innowacje oraz wspieranie inwestycji operatorów i dostawców w nowe funkcje bezpieczeństwa technicznego, związane również z takimi trendami, jak rzeczywistość rozszerzona i metawersum. W szczególności konieczne jest stworzenie europejskiej infrastruktury rozproszonych chmur obliczeniowych w oparciu o europejskie przepisy dotyczące takich kwestii, jak przechowywanie i przetwarzanie danych ([5]).

5.6. Szczególną uwagę należy poświęcić MŚP, które powinny mieć dostęp do programów finansowania zwiększających ich gotowość na cyberataki, a także do pomocy, szkoleń i programów edukacyjnych pomagających im zrozumieć ryzyko w cyberprzestrzeni i sposoby ochrony. UE powinna zapewnić mechanizm zachęt sprzyjający stopniowemu zapoznawaniu się z tą wiedzą w MŚP.

5.7. Komisja szacuje, że obecny niedobór wykwalifikowanej siły roboczej w dziedzinie cyberbezpieczeństwa wynosi pół miliona osób, a EKES docenia propozycję utworzenia Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Oczywiste jest, że wysiłki na szczeblu państw członkowskich nie wystarczają do zmniejszenia niedoboru kwalifikacji, dlatego Komitet sugeruje, by wraz z uruchomieniem Akademii Komisja wykorzystała dynamikę powstałą dzięki Europejskiemu Rokowi Umiejętności oraz by koordynowała i finansowała zakrojone na szeroką skalę programy szkoleniowe i programy kształcenia i szkolenia zawodowego na szczeblu UE, które zaangażują wszystkie państwa członkowskie i skoncentrują się na zapewnieniu wykwalifikowanej siły roboczej wszystkim agencjom i organom zaangażowanym w cyberobronę, a także prywatnym sieciom cywilnym. Szczególny nacisk należy położyć na szkolenie pracowników, szczególnie w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki (STEM).

5.8. Ponadto EKES uważa, że kluczowe znaczenie ma podnoszenie świadomości obywateli na temat cyberbezpieczeństwa, aby ograniczyć narażenie na cyberataki, zwłaszcza w odniesieniu do podstawowych cyberprzestępstw wymierzonych w ogół społeczeństwa. Wzywa do opracowania programów nauczania w dziedzinie cyberbezpieczeństwa i programów szkolenia w zakresie cyberbezpieczeństwa przez całe życie, które skupią się na poprawie umiejętności w dziedzinie cyberbezpieczeństwa oraz jego popularyzacji i zwiększaniu jego atrakcyjności w oczach obywateli, zwłaszcza młodszego pokolenia. EKES opowiada się za uwzględnianiem rozważań nad cyberbezpieczeństwem we wszystkich przyszłych politykach publicznych UE i informowaniem ogółu społeczeństwa o zagrożeniach cyberbezpieczeństwa, w tym za pomocą bezpłatnych programów szkoleniowych dla całej ludności, bezpłatnych aplikacji informacyjnych na telefony komórkowe oraz komunikatów emitowanych w porach największej oglądalności telewizji. Równolegle do tych działań należy dążyć do powszechnej zmiany postaw na każdym poziomie społeczeństwa, by przekonać je do podejścia ukierunkowanego na cyberbezpieczeństwo.

5.9. EKES uważa, że zasadnicze znaczenie mają ocena profili ryzyka dostawców oraz stosowanie odpowiednich ograniczeń wobec tych, których uznano za podmioty wysokiego ryzyka, w tym niezbędnych wyłączeń dotyczących kluczowych aktywów i aplikacji określonych jako krytyczne i wrażliwe w skoordynowanej ocenie ryzyka UE, a także certyfikacja zaufanych dostawców sprzętu i oprogramowania.

6. **Zawiązywanie partnerstw w celu sprostania wspólnym wyzwaniom**

6.1. Poziom gotowości poszczególnych państw członkowskich na przyszłe cyberataki znacznie się różni. EKES jest zdania, że natychmiastowym pierwszym krokiem jest utworzenie wewnątrzunijnej platformy komunikacyjnej dotyczącej najlepszych praktyk, w ramach której najbardziej zaawansowane w dziedzinie cyberprzestrzeni państwa członkowskie będą mogły dzielić się swoją wiedzą z innymi krajami i ułatwiać jej natychmiastowe wykorzystanie. Pomogłoby to zwiększyć wzajemne zaufanie między podmiotami krajowymi. Po drugie, Komitet uważa, że potrzebna jest ściślejsza współpraca między podmiotami państwowymi i niepaństwowymi w całej UE w celu poprawy cyberbezpieczeństwa produktów i usług na rynku wewnętrznym. Proponuje również utworzenie wspólnej unijnej platformy zgłaszania cyberincydentów, w tym unijnej czarnej listy wszystkich cybersprzestępców.

([5]) Np. francusko-niemiecka inicjatywa Gaia-X.

6.2. EKES jest zdania, że ścisła współpraca z sojusznikami NATO w dziedzinie wojskowej musi koncentrować się nie tylko na budowaniu zdolności i wczesnym wykrywaniu, lecz także na wspólnych projektach w zakresie badań, rozwoju i innowacji, wymianie najlepszych praktyk i wymianach między ekspertami, dużych programach szkoleniowych i symulacji cyberataków. Głównym celem powinno być rozszerzenie wspólnej zdolności reagowania i stworzenie synergii w celu przeciwdziałania przyszłym zagrożeniom hybrydowym, zgodnie ze wspólną deklaracją warszawską z 2016 r. i brukselską z 2018 r. We współpracy między UE a NATO nadal istnieje wiele aspektów, które można wykorzystać, a natychmiastowe postępy mogą rzeczywiście wpłynąć na zapewnienie bezpieczeństwa naszym obywatelom i społeczeństwom.

6.3. Komitet uważa, że dyskusje na szczeblu światowym i z naszymi partnerami międzynarodowymi powinny stworzyć warunki do promowania globalnej i otwartej cyberprzestrzeni, w której chroni się prawa człowieka, podstawowe wolności i praworządność, a także skupia się na opracowaniu wiążących standardów międzynarodowych w sektorach charakteryzujących się szybkim rozwojem cyfrowym. EKES zaleca wysokiemu przedstawicielowi dokonanie przeglądu istniejących dwustronnych dialogów w sprawach cyberprzestrzeni i podjęcie dalszych negocjacji z innymi państwami i odpowiednimi organizacjami międzynarodowymi w celu promowania globalnych ram stosowania prawa międzynarodowego w cyberprzestrzeni, w oparciu o ścisły warunek wzajemności.

6.4. Wreszcie Komitet jest zdania, że UE jest najlepiej przygotowana do prowadzenia międzynarodowych debat na temat przyszłości cyberbezpieczeństwa, zwłaszcza w ramach dyskusji ONZ, ze względu na jej solidne fundamenty w postaci podstawowych swobód demokratycznych. UE musi również zaangażować się w zwalczanie reżimów totalitarnych, które monitorują dane obywateli i naruszają ich prawa i wolności, oraz zdecydowanie sprzeciwiać się wszelkim systemom scoringu obywateli. EKES wyraźnie stwierdza, że prawdziwa demokracja nie może istnieć bez efektywnej ochrony danych osobowych, i uważa, że odpowiedzialne i skuteczne zarządzanie danymi ma kluczowe znaczenie dla przekształcenia hiperłączności w atut.

Bruksela, dnia 14 czerwca 2023 r.

Oliver RÖPKE
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego