Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie »Agencji UE ds. Bezpieczeństwa Cybernetycznego« ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa cybernetycznego w zakresie technologii informacyjno-komunikacyjnych (»akt ws. Bezpieczeństwa cybernetycznego«)”

[COM(2017) 477 final/2 2017/0225 (COD)]

(2018/C 227/13)

Sprawozdawca: **Alberto MAZZOLA**

Współsprawozdawca: **Antonio LONGO**

Konsultacja	Parlament Europejski, 23.10.2017
	Rada Unii Europejskiej, 25.10.2017
Podstawa prawna	Art. 114 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	5.2.2018
Data przyjęcia na sesji plenarnej	14.2.2018
Sesja plenarna nr	532
Wynik głosowania	206/1/2
(za/przeciw/wstrzymało się)	

1. **Wnioski i zalecenia**

1.1. EKES uważa, że nowy stały mandat ENISA zaproponowany przez Komisję Europejską przyczyni się znacznie do zwiększenia odporności europejskich systemów. Jednak towarzyszący temu tymczasowy budżet i zasoby przyznane agencji ENISA będą niewystarczające do wykonania przez nią mandatu.

1.2. EKES zaleca, aby wszystkie państwa członkowskie utworzyły wyraźny odpowiednik ENISA, gdyż większość z nich jeszcze tego nie uczyniła.

1.3. EKES jest również zdania, że pod względem budowania zdolności agencja ENISA powinna kłaść nacisk na działania wspierające administrację elektroniczną ([1]). Tożsamość cyfrowa osób, organizacji i przedmiotów w UE/na świecie ma kluczowe znaczenie, a priorytetem powinno być zapobieganie kradzieży tożsamości i oszustwom internetowym, a także ich zwalczanie.

1.4. EKES zaleca, by ENISA sporządzała regularne sprawozdania na temat cybergotowości państw członkowskich, koncentrując się głównie na sektorach wymienionych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji. W ramach corocznego europejskiego ćwiczenia w dziedzinie cyberbezpieczeństwa należy ocenić gotowość państw członkowskich oraz skuteczność europejskiego mechanizmu działania w odpowiedzi na kryzys cybernetyczny, a także sporządzić zalecenia.

1.5. EKES popiera propozycję stworzenia sieci eksperckiej dotyczącej cyberbezpieczeństwa, którą wspierałoby Europejskie Centrum Badań i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego. Mogłaby ona promować europejską suwerenność cyfrową poprzez tworzenie konkurencyjnej europejskiej bazy przemysłowej dla kluczowych zdolności technologicznych w oparciu o prace wykonane przez umowne partnerstwo publiczno-prywatne, które powinno rozwinąć się w trójstronne wspólne przedsięwzięcie.

1.6. Jedną z najważniejszych przyczyn incydentów cybernetycznych stanowi czynnik ludzki. Zdaniem EKES-u konieczne jest stworzenie solidnego zasobu umiejętności cybernetycznych oraz poprawienie higieny cyberbezpieczeństwa, również poprzez kampanie uświadamiające adresowane do indywidualnych osób i przedsiębiorstw. EKES popiera stworzenie certyfikowanego przez UE programu nauczania dla szkół średnich i dla wysoko wykwalifikowanych pracowników.

([1]) „Jednolity rynek cyfrowy: przegląd śródokresowy”.

1.7. EKES uważa, że europejski jednolity rynek cyfrowy wymaga także jednolitej interpretacji przepisów w zakresie cyberbezpieczeństwa, w tym wzajemnego uznawania między państwami członkowskimi, oraz że ramy i systemy certyfikacji dla różnorodnych sektorów mogłyby stanowić wspólny punkt odniesienia. Jednak poszczególnym sektorom trzeba zapewnić różne podejścia ze względu na ich sposób funkcjonowania. Dlatego też EKES uważa, że w procesie tym powinny uczestniczyć agencje sektorowe UE (EASA, ERA, EMA itd.) i że w niektórych przypadkach powinny one być, za zgodą ENISA dla zapewnienia spójności, delegowane do opracowania systemów certyfikacji bezpieczeństwa cybernetycznego. Minimalne europejskie standardy bezpieczeństwa IT należy przyjmować we współpracy z CEN/CENELEC/ETSI.

1.8. Planowana wspierana przez ENISA Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa powinna się składać z krajowych organów nadzoru ds. certyfikacji, podmiotów sektora prywatnego, w tym podmiotów z różnych domen zastosowań, oraz podmiotów naukowych i przedstawicieli społeczeństwa obywatelskiego.

1.9. EKES jest zdania, że w imieniu Komisji agencja powinna monitorować skuteczność i proces decyzyjny krajowych organów nadzoru ds. certyfikacji za pomocą audytów i inspekcji oraz że w rozporządzeniu powinny zostać określone zadania i sankcje w przypadku nieprzestrzegania norm.

1.10. EKES uważa, że działalność certyfikacyjna nie może wykluczać odpowiedniego systemu etykietowania, który byłby stosowany również w wypadku importowanych produktów w celu zwiększenia zaufania konsumentów.

1.11. Europa powinna zwiększyć skalę inwestycji, łącząc różne fundusze UE, fundusze krajowe i inwestycje sektora prywatnego z myślą o celach strategicznych w ramach dobrej współpracy publiczno-prywatnej, również poprzez stworzenie – w obecnym i przyszłym ramowym programie badań – funduszu na rzecz innowacji, badań i rozwoju w zakresie cyberbezpieczeństwa UE. Ponadto Europa powinna stworzyć fundusz na rzecz wdrażania cyberbezpieczeństwa, otwierając nowe możliwości w bieżącym i przyszłym instrumencie „Łącząc Europę", jak również w kolejnym EFIS 3.0.

1.12. EKES uważa, że minimalny poziom bezpieczeństwa jest niezbędny dla zwykłych urządzeń połączonych w ramach „internetu ludzi". W tym wypadku certyfikacja jest kluczową metodą zapewnienia wyższego poziomu bezpieczeństwa. Priorytetem powinno być bezpieczeństwo internetu rzeczy.

2. **Obecne ramy cyberbezpieczeństwa**

2.1. Cyberbezpieczeństwo ma bardzo istotne znaczenie zarówno dla dobrobytu i bezpieczeństwa narodowego, jak i dla samego funkcjonowania naszej demokracji, naszych swobód i wartości. W światowym indeksie cyberbezpieczeństwa ONZ stwierdza się, że „cyberbezpieczeństwo jest ekosystemem, w którym przepisy, organizacje, umiejętności i wdrażanie techniczne muszą pozostawać w harmonii ze sobą, by być skuteczne", i dodaje się, że cyberbezpieczeństwo „staje się coraz ważniejsze dla decydentów poszczególnych krajów".

2.2. Potrzeba bezpiecznego ekosystemu nabiera kluczowego znaczenia w związku z rewolucją internetową. Rewolucja ta nie tylko przedefiniowała sektory obejmujące relację między przedsiębiorstwem a konsumentem, takie jak media, usługi detaliczne i finansowe, lecz również zmienia charakter produkcji, energii, rolnictwa, transportu i innych sektorów przemysłowych gospodarki, które łącznie odpowiadają za nieomal dwie trzecie światowego produktu krajowego brutto, a także za infrastrukturę publiczną i interakcje obywateli z administracją publiczną.

2.3. Strategia jednolitego rynku cyfrowego opiera się na poprawie dostępu do towarów, usług i treści, tworzeniu odpowiednich ram prawnych dla sieci i usług cyfrowych oraz czerpaniu korzyści z gospodarki opartej na danych. Szacuje się, że co roku mogłaby ona wnieść do gospodarki UE 415 mld EUR. Przewiduje się, że niedobór wykwalifikowanej kadry w zakresie bezpieczeństwa cybernetycznego w sektorze prywatnym w Europie wyniesie w 2022 r. 350 tys. osób ([2]).

([2]) JOIN/2017/0450 final.

2.4. W badaniu z 2014 r. oszacowano, że w 2013 r. wpływ gospodarczy cyberprzestępczości w UE wyniósł 0,41 % PKB Unii (tzn. około 55 mld EUR) ([3]).

2.5. Według specjalnego badania Eurobarometru 464a dotyczącego postaw Europejczyków wobec cyberbezpieczeństwa 73 % użytkowników internetu jest zaniepokojonych, że strony internetowe mogą nie zapewniać bezpieczeństwa ich informacji personalnych w internecie, a 65 % – że mogą tego nie czynić władze publiczne. Większość respondentów wyraziła obawę, że może paść ofiarą różnych form cyberprzestępczości, szczególnie z powodu złośliwego oprogramowania na swych urządzeniach (69 %), kradzieży tożsamości (69 %) oraz oszustw związanych z kartami bankowymi i bankowością internetową (66 %) ([4]).

2.6. Do tej pory żadne ramy prawne nie nadążały za tempem innowacji cyfrowej, a szereg aktów prawnych przyczynia się do ustanowienia odpowiednich ram punkt po punkcie: przegląd Europejskiego kodeksu łączności elektronicznej, ogólne rozporządzenie o ochronie danych, dyrektywa w sprawie bezpieczeństwa sieci i informacji, rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS), Tarcza Prywatności UE–USA, dyrektywa w sprawie oszustw związanych z płatnościami bezgotówkowymi itd.

2.7. Oprócz ENISA, agencji UE ds. cyberbezpieczeństwa, istnieje wiele różnych organizacji zajmujących się kwestiami cyberbezpieczeństwa: Europol, CERT-UE (zespół reagowania na incydenty komputerowe), Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN UE), Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), ośrodek wymiany i analizy informacji (ISAC), Europejska Organizacja Cyberbezpieczeństwa (ECSO), Europejska Agencja Obrony (EDA), Centrum Doskonałości NATO ds. Współpracy w dziedzinie Obrony przed Atakami Cybernetycznymi i GGE ONZ (ONZ-owska grupa ekspertów rządowych ds. sytuacji w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego).

2.8. Uwzględnianie bezpieczeństwa na etapie projektowania ma kluczowe znaczenie dla zapewnienia wysokiej jakości towarów i usług: inteligentne urządzenia nie są aż tak inteligentne, jeżeli nie są zabezpieczone. To samo dotyczy inteligentnych samochodów, miast i szpitali, które wymagają wbudowanego bezpieczeństwa urządzeń, systemów, architektury i usług.

2.9. W dniach 19–20 października 2017 r. Rada Europejska zwróciła się o przyjęcie wspólnego podejścia do cyberbezpieczeństwa UE w następstwie proponowanego pakietu reform, postulując „wspólne podejście do cyberbezpieczeństwa: świat cyfrowy wymaga zaufania, które można zbudować tylko wtedy, gdy zapewnimy bardziej proaktywne uwzględnianie bezpieczeństwa na etapie projektowania we wszystkich politykach cyfrowych, zapewnimy odpowiednią certyfikację bezpieczeństwa dla produktów i usług oraz zwiększymy naszą zdolność w zakresie zapobiegania cyberatakom, ich powstrzymywania i wykrywania oraz reagowania na takie ataki" ([5]).

2.10. W swej rezolucji z 17 maja 2017 r. Parlament Europejski „podkreśla potrzebę zapewnienia pełnego bezpieczeństwa w całym łańcuchu wartości usług finansowych; zwraca uwagę na poważne i różnorodne zagrożenia stwarzane przez cyberataki na naszą infrastrukturę rynków finansowych, internet rzeczy, waluty i dane; […] wzywa europejskie urzędy nadzoru, by […] regularnie przeprowadzały przegląd istniejących norm operacyjnych obejmujących zagrożenia w zakresie ICT w instytucjach finansowych; ponadto apeluje, […], aby Europejski Urząd Nadzoru opracował wytyczne dotyczące monitorowania tych zagrożeń; zwraca uwagę na znaczenie fachowej wiedzy technicznej w europejskich urzędach nadzoru" ([6]).

2.11. EKES miał wcześniej kilka okazji do zajęcia się tą kwestią ([7]), m.in. podczas szczytu w Tallinie, na konferencji poświęconej przyszłemu rozwojowi administracji elektronicznej ([8]), i utworzył stałą grupę analityczną ds. agendy cyfrowej.

([3]) Dokument roboczy służb Komisji „Ocena skutków", towarzyszący wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady, część 1/6, s. 21, Bruksela, 13 września 2017 r.
([4]) Specjalny Eurobarometr 464a – Wave EB87.4 – „Postawy Europejczyków wobec cyberbezpieczeństwa", wrzesień 2017 r.
([5]) Konkluzje Rady Europejskiej z dnia 19 października 2017 r.
([6]) Rezolucja PE, 17 maja 2017 r. – A8-0176/2017.
([7]) „Jednolity rynek cyfrowy/przegląd śródokresowy", Dz.U. C 75 z 10.3.2017, s. 124, Dz.U. C 246 z 28.7.2017, s. 8, Dz.U. C 345 z 13.10.2017, s. 52, Dz.U. C 288 z 31.8.2017, s. 62, Dz.U. C 271 z 19.9.2013, s. 133.
([8]) Komunikat prasowy EKES-u nr 31/2017: Debata społeczeństwa obywatelskiego z przyszłą prezydencją estońską na temat e-administracji i bezpieczeństwa cybernetycznego: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incoming-estonianpresidency.

3. **Wnioski Komisji**

3.1. Pakiet w sprawie cyberbezpieczeństwa obejmuje wspólny komunikat stanowiący przegląd wcześniejszej strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego (2013 r.), a także akt ws. bezpieczeństwa cybernetycznego dotyczący nowego mandatu ENISA oraz proponowane ramy certyfikacji.

3.2. Strategia koncentruje się wokół trzech głównych elementów: odporności, prewencji i współpracy międzynarodowej. Część dotycząca prewencji skupia się głównie na kwestiach cyberprzestępczości, w tym na konwencji budapeszteńskiej, a część poświęcona współpracy międzynarodowej dotyczy cyberobrony, dyplomacji cyfrowej i współpracy z NATO.

3.3. We wniosku zaproponowano też nowe inicjatywy:

— budowę silniejszej agencji UE ds. cyberbezpieczeństwa;

— wprowadzenie ogólnounijnego systemu certyfikacji cyberbezpieczeństwa;

— szybkie wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji.

3.4. W części dotyczącej odporności zaproponowano działania związane z cyberbezpieczeństwem, skupiając się zwłaszcza na: kwestiach rynkowych, dyrektywie w sprawie bezpieczeństwa sieci i informacji, szybkim reagowaniu w sytuacjach kryzysowych, rozwijaniu kompetencji UE, kształceniu, szkoleniu – w zakresie umiejętności cybernetycznych i higieny cyberbezpieczeństwa – oraz podnoszeniu świadomości.

3.5. Równocześnie w akcie ws. bezpieczeństwa cybernetycznego zaproponowano stworzenie ram certyfikacji cyberbezpieczeństwa UE w odniesieniu do produktów i usług ICT.

3.6. W akcie ws. bezpieczeństwa cybernetycznego zaproponowano większą rolę dla ENISA jako agencji UE ds. cyberbezpieczeństwa, nadając jej stały mandat. Oczekuje się, że ENISA będzie oprócz swych obecnych obowiązków wykonywać nowe pomocnicze i koordynujące zadania związane ze wsparciem wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji, strategią Unii Europejskiej w zakresie cyberbezpieczeństwa, planem działania, budowaniem zdolności, wiedzą, informacją, podnoszeniem poziomu świadomości, zadaniami związanymi z rynkiem takimi jak wsparcie normalizacji i certyfikacji, badaniami naukowymi i innowacją, ogólnoeuropejskimi ćwiczeniami w tej dziedzinie (Cyber Europe) oraz sekretariatem sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

4. **Uwagi ogólne – przegląd**

4.1. ***Kontekst: odporność***

4.1.1. *Jednolity rynek cyberbezpieczeństwa*

Obowiązek dochowania należytej staranności: rozwinięcie proponowanej, wspomnianej we wspólnym komunikacie zasady „obowiązku dochowania należytej staranności" w celu zastosowania procesów bezpiecznego rozwoju cyklu życia jest ciekawą koncepcją, która musi zostać opracowana wspólnie z przemysłem UE i która mogłaby prowadzić do przyjęcia kompleksowego podejścia do zgodności z prawem UE. W przyszłych działaniach należy uwzględniać kwestię bezpieczeństwa domyślnego (*security by default*).

Odpowiedzialność: certyfikacja pomoże w obarczeniu odpowiedzialnością na wypadek sporu.

4.1.2. Dyrektywa w sprawie bezpieczeństwa sieci i informacji: energia, transport, bankowość/finanse, zdrowie, woda, infrastruktura cyfrowa, handel elektroniczny.

Zdaniem EKES-u pełne i skuteczne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji jest niezbędne do zapewnienia odporności krytycznych sektorów krajowych.

EKES uważa, że należy wzmocnić wymianę informacji między podmiotami publicznymi i prywatnymi za pośrednictwem ośrodków wymiany i analizy informacji (ISAC). Trzeba opracować odpowiedni mechanizm umożliwiający bezpieczną wymianę informacji w obrębie ISAC oraz między CSIRT a ISAC, w oparciu o ocenę/analizę obecnie stosowanego mechanizmu.

4.1.3. *Szybkie reagowanie w sytuacjach wyjątkowych*

Podejście oparte na planie działania stanowiłoby skuteczne narzędzie reagowania operacyjnego na incydenty na szeroką skalę na szczeblu UE i państw członkowskich. Komitet podkreśla potrzebę włączenia sektora prywatnego. Niezbędne jest uwzględnienie w mechanizmie reagowania operacyjnego operatorów usług kluczowych, gdyż mogą oni dostarczyć cennych informacji dotyczących zagrożeń lub zapewnić wsparcie w wykrywaniu zagrożeń i kryzysów toczących się na szeroką skalę, a także w reagowaniu na nie.

We wspólnym komunikacie zaproponowano włączenie cyberincydentów do mechanizmów zarządzania kryzysowego UE. Chociaż EKES rozumie potrzebę zbiorowej reakcji i solidarności na wypadek ataku, potrzebne jest lepsze zrozumienie, w jaki sposób można by je wprowadzić w życie, zważywszy że zagrożenia cybernetyczne zazwyczaj rozprzestrzeniają się w różnych krajach. Narzędzia stosowane w krajowych sytuacjach wyjątkowych można by jedynie częściowo zastosować w wypadku lokalnej potrzeby.

4.1.4. *Rozwijanie kompetencji UE*

Aby UE była rzeczywiście konkurencyjna na arenie międzynarodowej i zbudowała solidną bazę technologiczną, konieczne jest stworzenie spójnych, długofalowych ram obejmujących wszystkie etapy łańcucha wartości w zakresie cyberbezpieczeństwa. W tym względzie zasadnicze znaczenie dla rozwoju europejskiego łańcucha wartości w zakresie cyberbezpieczeństwa ma krzewienie współpracy między europejskimi ekosystemami regionalnymi. EKES przyjmuje z zadowoleniem propozycję stworzenia sieci eksperckiej dotyczącej cyberbezpieczeństwa.

Sieć mogłaby przyczynić się do europejskiej suwerenności cyfrowej poprzez rozwijanie konkurencyjnej europejskiej bazy przemysłowej i zmniejszenie zależności od know-how opracowanego poza UE odnośnie do kluczowych zdolności technologicznych, organizować ćwiczenia techniczne, warsztaty, a nawet niezbędne szkolenie z zakresu higieny cyberbezpieczeństwa dla wysoko wykwalifikowanych pracowników i użytkowników nieprofesjonalnych oraz – na podstawie prac cPPP – wspomóc opracowanie sieci krajowych organizacji publiczno-prywatnych w celu rozwinięcia rynku w Europie. „Rozwijanie cPPP powinno prowadzić do optymalizacji, dostosowania lub ekspansji" (Program prac trzech prezydencji EE-BD-AT w dziedzinie cyberbezpieczeństwa) za pomocą ustanowienia trójstronnego wspólnego przedsięwzięcia (Komisja, państwa członkowskie, przedsiębiorstwa).

By osiągnąć skuteczność i proponowane cele na szczeblu europejskim, sieć musi polegać na dobrze określonym systemie zarządzania.

Europejskie Centrum Badań i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego służyłoby jej wsparciem na szczeblu europejskim, łącząc istniejące krajowe ośrodki kompetencji w całej UE. Nie tylko koordynowałoby ono badania naukowe i zarządzało nimi podobnie jak w innych wspólnych przedsięwzięciach, lecz umożliwiłoby również skuteczny rozwój europejskiego ekosystemu cyberbezpieczeństwa, który wspomagałby wdrażanie i stosowanie innowacji UE.

4.2. ***Kontekst: prewencja***

4.2.1. Zwalczanie cyberprzestępczości jest priorytetem na szczeblach krajowym i europejskim, który wymaga silnego zaangażowania politycznego. Prewencja powinna być prowadzona w oparciu o silne partnerstwo sektora publicznego i prywatnego, umożliwiające skuteczną wymianę informacji i wiedzy fachowej na szczeblu krajowym i europejskim. Można by przewidzieć możliwości poszerzenia działalności Europolu w dziedzinie informatyki śledczej i monitorowania.

4.3. ***Kontekst: współpraca międzynarodowa***

4.3.1. Rozwijanie i podtrzymywanie opartej na zaufaniu współpracy z państwami trzecimi za pomocą dyplomacji cyfrowej i partnerstw biznesowych ma kluczowe znaczenie dla umocnienia zdolności Europy do zapobiegania cyberatakom na dużą skalę i reagowania na nie. Europa powinna pogłębiać współpracę z USA, Chinami, Izraelem, Indiami i Japonią. Modernizacja kontroli eksportu UE nie powinna dopuszczać do łamania praw człowieka czy też nieprawidłowego używania technologii w sposób zagrażający bezpieczeństwu UE, lecz powinna również gwarantować, że przemysł UE nie będzie miał gorszej pozycji w stosunku do ofert państw trzecich. Należy przewidzieć strategię ad hoc dla krajów przystępujących w celu przygotowania się do wymiany wrażliwych transgranicznych danych, w tym możliwość udziału, w charakterze obserwatorów, w niektórych działaniach ENISA. Kraje te powinny być klasyfikowane według ich gotowości do zwalczania cyberprzestępczości, można by też rozważyć stworzenie „czarnej listy".

4.3.2. EKES przyjmuje z zadowoleniem wprowadzenie cyberobrony w planowanej drugiej fazie budowy ewentualnego centrum kompetencji UE w dziedzinie cyberbezpieczeństwa. Dlatego też Europa mogłaby tymczasem przeanalizować rozwój umiejętności podwójnego zastosowania, w tym wykorzystanie Europejskiego Funduszu Obronnego oraz planowane utworzenie do 2018 r. platformy szkolenia i kształcenia w dziedzinie cyberobrony. Zważywszy na wzajemnie uznawany potencjał i zagrożenia, EKES uważa za konieczne rozwijanie współpracy UE–NATO. Europejski przemysł powinien też uważnie śledzić rozwój sytuacji w zakresie współpracy UE–NATO dotyczącej większej interoperacyjności standardów cyberbezpieczeństwa oraz innych form współpracy w kontekście podejścia UE do cyberobrony.

4.4. ***Unijne ramy certyfikacji***

4.4.1. EKES uważa, że Europa musi stawić czoła wyzwaniu fragmentacji cyberbezpieczeństwa poprzez jednolitą interpretację przepisów, w tym wzajemne uznawanie między państwami członkowskimi w ujednoliconych ramach w celu ułatwienia ochrony jednolitego rynku cyfrowego. Ramy certyfikacji mogą stanowić wspólny punkt odniesienia (w razie potrzeby wraz ze szczególnymi uregulowaniami na wyższych szczeblach), zapewniając synergię we wszystkich sektorach wertykalnych i zmniejszając obecną fragmentację.

4.4.2. EKES przyjmuje z zadowoleniem stworzenie unijnych ram certyfikacji cyberbezpieczeństwa oraz systemów certyfikacji cyberbezpieczeństwa dla różnych sektorów w oparciu o odpowiednie wymogi i we współpracy z głównymi zainteresowanymi stronami. Jednak czas potrzebny na wprowadzenie na rynek produktów, koszty certyfikacji, jakość i bezpieczeństwo to najważniejsze elementy, które należy wziąć pod uwagę. Systemy certyfikacji zostaną stworzone z myślą o zwiększeniu bezpieczeństwa stosownie do obecnych potrzeb i wiedzy o zagrożeniach: należy mieć na uwadze ich elastyczność oraz zdolność ewolucji, tak aby można było dokonywać koniecznych aktualizacji. Poszczególnym sektorom trzeba zapewnić różne podejścia ze względu na ich sposób funkcjonowania. Dlatego też EKES uważa, że w procesie tym powinny uczestniczyć agencje sektorowe UE (EASA, EUNB, ERA, EMA itd.) i że w niektórych przypadkach powinny one być – za zgodą ENISA w celu zapewnienia spójności i uniknięcia powielania – delegowane do opracowania systemów certyfikacji cyberbezpieczeństwa.

4.4.3. Zdaniem Komitetu istotne jest oparcie ram certyfikacji na wspólnie określonych europejskich standardach cyberbezpieczeństwa i ICT, które w miarę możliwości powinny zostać uznane na szczeblu międzynarodowym. Wziąwszy pod uwagę ramy czasowe i krajowe prerogatywy, należy we współpracy z CEN/CENELEC/ETSI przyjąć minimalne standardy europejskie dotyczące bezpieczeństwa IT. Trzeba odnieść się pozytywnie do standardów zawodowych, lecz nie powinny być one prawnie wiążące czy też utrudniać konkurencji.

4.4.4. Istnieje wyraźnie potrzeba powiązania zobowiązań z różnymi poziomami pewności w oparciu o wpływ zagrożeń. Zapoczątkowanie dialogu z przedsiębiorstwami ubezpieczeniowymi mogłoby być korzystne z punktu widzenia przyjęcia skutecznych wymogów cyberbezpieczeństwa zgodnie z dziedziną zastosowania. Zdaniem EKES-u konieczne jest wspieranie i zachęcanie przedsiębiorstw dążących do „wysokiego poziomu pewności", zwłaszcza w odniesieniu do krytycznych dla życia urządzeń i systemów.

4.4.5. Biorąc pod uwagę czas, jaki upłynął od momentu przyjęcia dyrektywy 85/374/EWG ([9]), oraz najnowszy postęp technologiczny, EKES wnosi, by Komisja zbadała przydatność włączenia w zakres tej dyrektywy niektórych scenariuszy określonych w omawianym wniosku dotyczącym rozporządzenia, z myślą o zapewnieniu bezpieczniejszych produktów o wysokim poziomie ochrony.

4.4.6. EKES uważa, że planowana Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa wspierana przez ENISA powinna się składać z krajowych organów nadzoru ds. certyfikacji, podmiotów sektora prywatnego i podmiotów z różnych domen zastosowań, tak by zapewnić opracowanie kompleksowych systemów certyfikacji. Ponadto należy zaplanować współpracę między nią a stowarzyszeniami przedstawicielskimi tego sektora z UE/EOG (np. cPPP, bankowość, transport, energia, federacje itd.) poprzez wyznaczenie ekspertów. Powinna ona być również w stanie wziąć pod uwagę europejskie osiągnięcia w dziedzinie certyfikacji (głównie w oparciu o umowę o wzajemnym uznaniu grupy wysokiej rangi urzędników ds. bezpieczeństwa systemów informatycznych, krajowe i zamknięte systemy) i mieć na celu utrzymanie europejskich przewag konkurencyjnych.

([9]) Dz.U. L 210 z 7.8.1985, s. 29.

4.4.7. EKES proponuje, by wraz z Komisją Europejską ta grupa zainteresowanych stron odpowiadała za wspólne opracowywanie systemów certyfikacji. Konieczne jest również określenie wymogów sektorowych na mocy konsensualnego porozumienia między podmiotami prywatnymi i publicznymi (użytkownikami i dostawcami).

4.4.8. Ponadto grupa powinna dokonywać regularnego przeglądu systemów certyfikacji, wziąwszy pod uwagę wymogi każdego sektora, i w razie konieczności dostosować systemy.

4.4.9. EKES popiera stopniowe znoszenie krajowych systemów certyfikacji na etapie wprowadzania europejskiego systemu, zgodnie z propozycją zawartą w art. 49 rozporządzenia. Jednolity rynek nie może działać w oparciu o różne, konkurencyjne wobec siebie przepisy krajowe. W tym celu EKES proponuje sporządzenie spisu wszystkich programów krajowych.

4.4.10. EKES proponuje, aby Komisja zainicjowała działania w celu promowania certyfikacji i certyfikatów cyberbezpieczeństwa w UE oraz w celu wspierania ich uznawania we wszystkich międzynarodowych umowach handlowych.

4.5. ***ENISA***

4.5.1. EKES uważa, że nowy stały mandat ENISA zaproponowany przez Komisję Europejską przyczyni się znacznie do zwiększenia odporności europejskich systemów. Jednak towarzyszący temu tymczasowy budżet i zasoby przyznane zreformowanej agencji ENISA mogą być niewystarczające do wykonania przez nią mandatu.

4.5.2. EKES zachęca wszystkie państwa członkowskie, aby utworzyły wyraźny, zbliżony odpowiednik ENISA, gdyż większość z nich jeszcze tego nie uczyniła. Należy wprowadzić zorganizowany program oddelegowywania ekspertów krajowych do agencji ENISA, aby sprzyjać wymianie najlepszych praktyk i wzmacniać zaufanie. Komitet zaleca też, by Komisja zadbała o gromadzenie i wymianę sprawdzonych rozwiązań i skutecznych środków działania istniejących obecnie w państwach członkowskich.

4.5.3. EKES jest ponadto zdania, że pod względem budowania zdolności agencja ENISA powinna kłaść nacisk na działania wspierające administrację elektroniczną ([10]). Tożsamość cyfrowa osób, organizacji, przedsiębiorstw i przedmiotów w UE/na świecie ma kluczowe znaczenie, a priorytetem powinno być zapobieganie kradzieży tożsamości i oszustwom internetowym oraz ich zwalczanie, a także przeciwdziałanie kradzieży przemysłowej własności intelektualnej.

4.5.4. ENISA powinna również sporządzać regularne sprawozdania na temat cybergotowości państw członkowskich, koncentrując się głównie na sektorach wymienionych w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji. W ramach corocznego europejskiego ćwiczenia w dziedzinie bezpieczeństwa cybernetycznego należy ocenić gotowość państw członkowskich oraz skuteczność europejskiego mechanizmu działania w odpowiedzi na kryzys cybernetyczny, a także sporządzić zalecenia.

4.5.5. EKES wyraża zaniepokojenie, że zasoby są zbyt ograniczone odnośnie do współpracy operacyjnej, w tym sieci CSIRT.

4.5.6. Jeżeli chodzi o zadania związane z rynkiem, EKES uważa, że rozwój współpracy z państwami członkowskimi i ustanowienie formalnej sieci agencji cyberbezpieczeństwa pomogłyby we współpracy zainteresowanych stron ([11]). Czas wejścia na rynek jest bardzo krótki, przedsiębiorstwa UE muszą być w stanie konkurować w tej dziedzinie i ENISA musi być w stanie stosownie reagować. EKES uważa, że ENISA – podobnie jak inne agencje UE – mogłaby zastosować w przyszłości system opłat i należności. EKES jest zaniepokojony, że konkurencja o umiejętności między UE a agencjami krajowymi mogłaby, podobnie jak to miało miejsce w innych dziedzinach, opóźnić właściwe ustanowienie ram regulacyjnych UE i zaszkodzić jednolitemu rynkowi UE.

4.5.7. EKES odnotowuje, że zadania dotyczące badań i innowacji oraz współpracy międzynarodowej są obecnie ograniczone do minimum.

([10]) „Jednolity rynek cyfrowy: przegląd śródokresowy".
([11]) Dz.U. C 75 z 10.3 2017, s. 124.

4.5.8. EKES uważa, że cyberbezpieczeństwo powinno być stałym przedmiotem dyskusji podczas wspólnych regularnych posiedzeń agencji z dziedziny wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW) oraz że ENISA i Europol powinny ze sobą systematycznie współpracować.

4.5.9. Ze względu na to, że świat cybernetyki jest bardzo innowacyjny, trzeba uważnie rozważyć standardy w celu uniknięcia przeszkód w innowacji, co wymaga dynamicznych ram. Należy w miarę możliwości zapewnić zarówno kompatybilność w przód, jak i wsteczną, by chronić inwestycje obywateli i przedsiębiorstw.

4.5.10. Ze względu na znaczenie krajowych organów nadzoru ds. certyfikacji EKES proponuje, by w rozporządzeniu ustanowiono już formalną sieć organów upoważnionych do rozwiązywania kwestii transgranicznych z pomocą ENISA. Sieć powinna się na późniejszym etapie przekształcić w jedną agencję.

4.5.11. Zaufanie ma fundamentalne znaczenie, lecz ENISA nie może wydawać decyzji czy też kontrolować sprawozdań. EKES jest zdania, że agencja powinna w imieniu Komisji monitorować skuteczność i proces decyzyjny krajowych organów nadzoru ds. certyfikacji za pomocą audytów i inspekcji.

4.5.12. Udział w zarządzie agencji ENISA należałoby rozszerzyć, tak aby objąć organizacje sektorowe i konsumenckie, które miałyby charakter obserwatorów.

4.6. ***Przemysł, MŚP, finansowanie/inwestycje i innowacyjne modele biznesowe***

4.6.1. *Przemysł i inwestycje*

By zwiększyć globalną konkurencyjność przedsiębiorstw UE działających w dziedzinie ICT, działania muszą być ukierunkowane na lepsze wsparcie wzrostu i konkurencyjności przemysłu ICT, w tym MŚP.

Europa powinna zwiększyć skalę inwestycji, łącząc różne fundusze UE, fundusze krajowe i inwestycje sektora prywatnego z myślą o celach strategicznych w ramach dobrej współpracy publiczno-prywatnej. Konieczne jest podniesienie poziomu inwestycji w kluczowych dziedzinach oraz wsparcie ich poprzez utworzenie – w obecnym i przyszłym ramowym programie badań – funduszu na rzecz innowacji, badań i rozwoju w zakresie cyberbezpieczeństwa UE. Ponadto Europa powinna stworzyć fundusz na rzecz wdrażania cyberbezpieczeństwa, otwierając nowe możliwości w bieżącym i przyszłym instrumencie „Łącząc Europę", jak również w kolejnym EFIS 3.0.

Należy stworzyć zachęty dla państw członkowskich UE, by w miarę możliwości zakupywały europejskie rozwiązania i wybierały europejskich dostawców, jeżeli są dostępni, zwłaszcza w wypadku wrażliwych zastosowań. Europa powinna wspierać rozwój europejskich liderów cyberprzestrzeni, którzy mogliby konkurować na światowym rynku.

4.6.2. *MŚP*

Ze względu na fragmentację rynku potrzebna jest większa jasność co do popytu ze strony klientów, by lepiej zająć się kwestią rynku. Bez zorganizowanego popytu – MŚP i przedsiębiorstwa typu start-up nie mogą się szybko rozwijać. W tym kontekście korzystne byłoby ustanowienie europejskiego centrum cyberbezpieczeństwa dla MŚP.

Technologia w zakresie cyberbezpieczeństwa szybko się zmienia, a MŚP mogą dzięki swej sprawności zapewnić zaawansowane rozwiązania potrzebne do utrzymania konkurencyjności. W porównaniu z państwami trzecimi UE nadal poszukuje odpowiedniego modelu biznesowego dla MŚP.

Można by opracować specjalne programy przeznaczone dla MŚP i przedsiębiorstw typu start-up, aby wesprzeć je w pokryciu kosztów certyfikacji i w ten sposób łagodzić ich ogromne trudności w gromadzeniu funduszy na własny rozwój technologiczny i handlowy.

4.7. ***Czynnik ludzki: kształcenie i ochrona***

4.7.1. EKES odnotowuje, że wniosek Komisji nie uwzględnia należycie człowieka jako siły napędowej procesów cyfrowych: ani jako beneficjenta, ani jako przyczyny głównych incydentów informatycznych.

4.7.2. Konieczne jest stworzenie solidnego zasobu umiejętności cybernetycznych oraz poprawienie higieny cyberbezpieczeństwa i zwiększenie świadomości pośród indywidualnych osób i przedsiębiorstw. By osiągnąć taki wynik, trzeba wziąć pod uwagę specjalne inwestycje, czas na szkolenie wysokiej klasy instruktorów, a także skuteczne kampanie uświadamiające. Wdrożenie tych trzech linii działania wymaga włączenia władz krajowych i regionalnych (odpowiedzialnych za ustanowienie skutecznych programów edukacyjnych i zainwestowanie w nie) oraz przedsiębiorstw i MŚP w zbiorowe podejście.

4.7.3. Należy zaplanować stworzenie ewentualnego programu nauczania certyfikowanego przez UE dla szkół średnich i wysoko wykwalifikowanych pracowników z aktywnym udziałem ENISA i jej krajowych odpowiedników. Ponadto przy opracowywaniu programów edukacyjnych należy mieć na uwadze równouprawnienie płci w celu poprawienia poziomu zatrudnienia w dziedzinie cyberbezpieczeństwa.

4.7.4. EKES uważa, że certyfikacja powinna obejmować odpowiedni system etykietowania, odnośnie do zarówno do sprzętu, jak i do oprogramowania, podobnie jak to ma miejsce w wypadku wielu innych produktów (np. w odniesieniu do produktów związanych z energią). Taki instrument przyniesie trojakie korzyści: ograniczenie kosztów dla przedsiębiorstw, wyeliminowanie obecnej fragmentacji rynku związanej z różnymi systemami certyfikacji przyjętymi już na szczeblu krajowym oraz ułatwienie konsumentom zrozumienia jakości i cech nabytego przedmiotu. W związku z tym istotne jest, by również produkty importowane z państw trzecich podlegały tym samym mechanizmom certyfikacji i etykietowania. Wreszcie, EKES jest zdania, że stworzenie doraźnego logo mogłoby ułatwić bezzwłoczne przekazywanie konsumentom i użytkownikom informacji o niezawodności nabywanych produktów czy też stron internetowych, na których prowadzone są transakcje lub przekazywane są wrażliwe dane.

4.7.5. ENISA powinna przyjąć na siebie odpowiedzialność za niezbędne działania informacyjne i uświadamiające na wielu szczeblach, tak by zwiększyć świadomość na temat bezpiecznych zachowań cyfrowych i zaufanie użytkowników do internetu. W tym celu należałoby zaangażować stowarzyszenia przedsiębiorstw i organizacje konsumenckie oraz inne organizacje działające w zakresie usług cyfrowych.

4.7.6. Zgodnie ze swoją propozycją zawartą już w opinii INT/828 EKES uważa, że w uzupełnieniu do aktu ws. bezpieczeństwa cybernetycznego istotne jest jak najszybsze uruchomienie kompleksowego europejskiego programu kształcenia i szkolenia w zakresie umiejętności cyfrowych w celu zagwarantowania wszystkim obywatelom narzędzi do jak najlepszego radzenia sobie z przemianami. Choć EKES jest świadomy szczególnych krajowych kompetencji w tej dziedzinie, ma zwłaszcza nadzieję, że program ten zostanie zapoczątkowany w szkołach i pozwoli na zwiększenie wiedzy nauczycieli, dostosowanie programów nauczania i dydaktyki do technologii cyfrowych (w tym e-learningu) i zapewni wszystkim uczniom szkolenie wysokiej jakości. Będzie miał on naturalne przedłużenie w uczeniu się przez całe życie w celu zmiany lub podniesienia kwalifikacji wszystkich pracowników ([12]).

5. **Uwagi szczegółowe**

5.1. ***Powstające technologie i rozwiązania: przypadek internetu rzeczy***

Liczba odbiorników hybrydowych wciąż rośnie i oczekuje się, że będzie wynosić wielokrotność liczby mieszkańców ziemi w związku z cyfryzacją komponentów, systemów i rozwiązań, a także wzmocnioną łącznością. Ten trend stwarza nowe możliwości dla cyberprzestępców, szczególnie dlatego, że urządzenia połączone w ramach internetu rzeczy często nie są objęte tak dobrą ochroną jak tradycyjne urządzenia.

Europejskie normy bezpieczeństwa w różnych pionach z użyciem urządzeń połączonych w ramach internetu rzeczy mogą ograniczyć wysiłki na rzecz rozwoju, czas i budżet dla wszystkich podmiotów przemysłowych w łańcuchu wartości połączonych produktów.

Prawdopodobne jest, że pewna forma minimalnego poziomu bezpieczeństwa za pomocą IAM (systemu zarządzania uprawnieniami i tożsamością użytkowników), wstawiania poprawek i zarządzania urządzeniami będzie niezbędna dla zwykłych urządzeń połączonych w ramach internetu ludzi. Ponieważ certyfikacja jest zasadniczą metodą zapewnienia wyższego poziomu bezpieczeństwa, w ramach nowego podejścia UE do certyfikacji trzeba położyć większy nacisk na bezpieczeństwo internetu rzeczy.

Bruksela, dnia 14 lutego 2018 r.

Georges DASSIS
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego

([12]) „Jednolity rynek cyfrowy: przegląd śródokresowy".