KOMISJA
EUROPEJSKA

Bruksela, dnia 5.7.2016 r.
COM(2016) 410 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego

1. WPROWADZENIE / KONTEKST

Incydenty w sferze bezpieczeństwa cybernetycznego codziennie powodują poważne szkody gospodarcze dla europejskich przedsiębiorstw i całej gospodarki i podważają zaufanie obywateli i przedsiębiorstw do społeczeństwa cyfrowego. Kradzież tajemnic przedsiębiorstwa, informacji handlowych i danych osobowych, zakłócanie świadczenia usług, w tym podstawowych, jak również zakłócanie funkcjonowania infrastruktury powoduje straty ekonomiczne rzędu setek miliardów euro rocznie[1]. Mogą one również pociągać za sobą konsekwencje dla praw podstawowych i społeczeństwa jako całości.

Strategia Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego[2] z 2013 r. (unijna strategia w zakresie bezpieczeństwa cybernetycznego) oraz jej główny rezultat: dyrektywa w sprawie bezpieczeństwa sieci i informacji[3], która ma zostać wkrótce przyjęta, jak również dyrektywa 2013/40/UE dotycząca ataków na systemy informatyczne, stanowią jak dotąd podstawową odpowiedź polityczną Unii Europejskiej na te wyzwania w dziedzinie bezpieczeństwa cybernetycznego. Ponadto UE ma również do dyspozycji wyspecjalizowane podmioty, takie jak: Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu i zespół reagowania na incydenty komputerowe (CERT-UE). Niedawno podjęto także szereg inicjatyw sektorowych (np. w dziedzinie energii i transportu), mających na celu zwiększenie bezpieczeństwa cybernetycznego w różnych sektorach krytycznych.

Pomimo tych pozytywnych osiągnięć UE pozostaje podatna na incydenty cybernetyczne, które mogą zagrażać jednolitemu rynkowi cyfrowemu oraz całemu życiu gospodarczemu i społecznemu. Ich wpływ może również wykraczać poza gospodarkę – w przypadku zagrożeń hybrydowych[4] ataki cybernetyczne mogą być stosowane w sposób skoordynowany z innymi działaniami w celu destabilizowania państwa lub rzucania wyzwań instytucjom politycznym.

W tych warunkach postępowanie z poważnym incydentem cybernetycznym dotyczącym jednocześnie wielu państw członkowskich może być dla UE niezwykle trudnym wyzwaniem. Dlatego też Komisja, biorąc również pod uwagę komunikaty dotyczące przeciwdziałania zagrożeniom hybrydowym oraz realizacji Europejskiej agendy bezpieczeństwa[5], szuka sposobów radzenia sobie ze zmieniającą się rzeczywistością w dziedzinie bezpieczeństwa cybernetycznego i ocenia dodatkowe środki, które mogą być potrzebne, aby zwiększyć odporność UE pod względem bezpieczeństwa cybernetycznego oraz usprawnić reagowanie na incydenty.

Ponadto Komisja zajmuje się również kwestią zdolności przemysłowych Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego. Chociaż Europa być może nie opanowała jeszcze całego łańcucha wartości technologii cyfrowych, konieczne jest przynajmniej

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*; Centrum Studiów Strategicznych i Międzynarodowych; czerwiec 2014.
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

utrzymanie i rozwijanie pewnych podstawowych zdolności. Dostarczanie produktów i usług, które zapewniają najwyższy poziom bezpieczeństwa cybernetycznego, jest ważną szansą dla branży bezpieczeństwa cybernetycznego w Europie i mogłoby stać się silną przewagą konkurencyjną. Oczekuje się, że globalny rynek bezpieczeństwa cybernetycznego będzie jednym z najszybciej rozwijających się segmentów sektora technologii informacyjno-komunikacyjnych (ICT)[6]. Dążeniu do uczynienia z UE lidera w tej dziedzinie musi towarzyszyć silna kultura bezpieczeństwa danych, w tym danych osobowych, i skutecznego reagowania na incydenty. Będzie to mocnym argumentem przemawiającym za inwestowaniem w UE i przyczyni się do osiągnięcia ambitnych celów jednolitego rynku cyfrowego w zakresie wzrostu gospodarczego i zatrudnienia.

Do zrealizowania powyższych zamiarów potrzebne jest silne zaangażowanie polityczne, w szczególności poprzez:

(i) zintensyfikowanie współpracy w celu zwiększenia gotowości i reagowania na incydenty cybernetyczne

Należy wzmocnić istniejące i uzgodnione mechanizmy współpracy, aby zwiększyć odporność i gotowość UE, w tym pod względem ewentualnego ogólnoeuropejskiego kryzysu w dziedzinie bezpieczeństwa cybernetycznego. Te mechanizmy współpracy powinny być kompleksowe i powinny obejmować cykl życia incydentu od zapobiegania do ścigania sprawców. Dla skutecznej współpracy między państwami członkowskimi i praktycznego wdrożenia wymogów dotyczących bezpieczeństwa w odniesieniu do krytycznych podmiotów niezbędne będzie również opracowanie przez ten sektor solidnych rozwiązań technicznych.

Jednocześnie zapewnienie odporności krytycznych zasobów cybernetycznych w całej Unii Europejskiej będzie wymagało ciągłych starań na rzecz znalezienia synergii międzysektorowych oraz uwzględnienia wymogów dotyczących bezpieczeństwa cybernetycznego we wszystkich odnośnych obszarach polityki UE. W tym celu w najbliższej przyszłości konieczna może być aktualizacja unijnej strategii w zakresie bezpieczeństwa cybernetycznego z 2013 r.

(ii) pokonywanie wyzwań stojących przed jednolitym rynkiem bezpieczeństwa cybernetycznego Europy

W strategii jednolitego rynku cyfrowego[7] przyznano, że wciąż istnieją pewne luki w szybko rozwijającej się dziedzinie technologii i rozwiązań w zakresie bezpieczeństwa sieci. Jednocześnie badania rynkowe wskazują na to, że rynek wewnętrzny UE jest nadal podzielony geograficznie pod względem dostarczania produktów i usług z branży bezpieczeństwa cybernetycznego[8]. W niniejszym komunikacie określono szereg środków polityki rynkowej mających na celu zlikwidowanie tych luk i sprostanie wyzwaniom w odniesieniu do jednolitego rynku.

[6] Zob. SWD(2016) 216.
[7] COM(2015) 192.
[8] Zob. SWD(2016) 216.

(iii) rozwijanie zdolności przemysłowych w dziedzinie bezpieczeństwa cybernetycznego

W strategii UE w zakresie bezpieczeństwa cybernetycznego, jak również w strategii jednolitego rynku cyfrowego, Komisja zobowiązała się do propagowania wzrostu podaży produktów i usług ze strony unijnego sektora bezpieczeństwa cybernetycznego. W związku z tym Komisja przyjmuje także decyzję torującą drogę ustaleniom umownym dotyczącym partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego, które to partnerstwo ma na celu wspieranie realizacji nowatorskiego europejskiego programu badań naukowych i innowacji w zakresie bezpieczeństwa cybernetycznego na rzecz większej konkurencyjności.

2. PRZECHODZENIE NA WYŻSZY POZIOM WSPÓŁPRACY, WIEDZY I ZDOLNOŚCI

Unijna strategia w zakresie bezpieczeństwa cybernetycznego, a w szczególności przyszła dyrektywa w sprawie bezpieczeństwa sieci i informacji[9], utoruje drogę lepszej współpracy państw członkowskich na poziomie UE. Szybkie i skuteczne wykonanie tej dyrektywy będzie miało kluczowe znaczenie z uwagi na rosnącą cyfryzację życia gospodarczego i społecznego (uwzględniając również chmurę, internet rzeczy i komunikację między urządzeniami), rosnącą skalę wzajemnych połączeń transgranicznych i szybko zmieniającą się sytuację w zakresie zagrożenia cybernetycznego[10]. W związku z tym UE musi przygotować się na możliwość zaistnienia kryzysu cybernetycznego[11] na dużą skalę, w tym na przykład poważnych jednoczesnych ataków na krytyczne systemy informacyjne w kilku państwach członkowskich[12].

Współpraca unijna jest zatem niezbędna, aby móc poradzić sobie zarówno z incydentami cybernetycznymi o mniejszej skali, które jednak mogą się rozprzestrzeniać, jak i z ewentualnym atakiem cybernetycznym na dużą skalę w wielu państwach członkowskich. Unia Europejska musi włączyć aspekty bezpieczeństwa cybernetycznego do istniejących mechanizmów zarządzania kryzysowego. Musi ona również zapewnić mechanizmy skutecznej współpracy i szybkiej wymiany informacji między sektorami i państwami członkowskimi na potrzeby reagowania na takie incydenty i zapobiegania im. Ponadto mechanizmy te powinny działać jak jeden spójny system bezpieczeństwa cybernetycznego i zwalczania cyberprzestępczości, pomagający państwom członkowskim lepiej współpracować w walce z terroryzmem, przestępczością zorganizowaną i cyberprzestępczością. Zwiększyłoby to również zdolność UE do koordynowania działań z partnerami międzynarodowymi w celu skutecznego reagowania na zagrożenia i incydenty o wymiarze globalnym.

[9] Zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji państwa członkowskie będą miały obowiązek zidentyfikować szereg podmiotów świadczących podstawowe usługi w takich dziedzinach, jak: energetyka, transport, finanse i zdrowie, uwzględnić ryzyko w zakresie bezpieczeństwa cybernetycznego, jak również zapewnić, aby określeni dostawcy usług cyfrowych zastosowali właściwe środki w celu wyeliminowania tego ryzyka.
[10] Zob. SWD(2016) 216.
[11] Zob. np. sprawozdanie ENISA: *Common practices of EU-level crisis management and applicability to cyber crises* (kwiecień 2016 r.).
[12] Zob. SWD(2016) 216.

2.1. Maksymalne wykorzystanie mechanizmów współpracy w zakresie bezpieczeństwa sieci i informacji oraz przejście na ENISA 2.0

Zasadniczym elementem zdolności krajowych wymaganych w dyrektywie w sprawie bezpieczeństwa sieci i informacji są Zespoły Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT), które odpowiadają za szybkie reagowanie na zagrożenia i incydenty cybernetyczne. Utworzą one sieć CSIRT, aby promować skuteczną współpracę operacyjną w zakresie konkretnych incydentów w sferze bezpieczeństwa cybernetycznego i wymianę informacji o ryzyku. Ponadto na mocy dyrektywy ustanowiona zostanie grupa na rzecz współpracy między państwami członkowskimi, której celem będzie wspieranie i ułatwianie współpracy strategicznej oraz budowanie zaufania między państwami.

Biorąc pod uwagę charakter i mnogość zagrożeń cybernetycznych, Komisja zachęca państwa członkowskie do maksymalnego wykorzystania mechanizmów współpracy w zakresie bezpieczeństwa sieci i informacji, które są obecnie do ich dyspozycji, a także do zacieśnienia współpracy transgranicznej związanej z gotowością na wypadek poważnego incydentu cybernetycznego. W ramach takiej dodatkowej współpracy w zakresie poważnego incydentu cybernetycznego przydatne byłoby stosowanie skoordynowanego podejścia do współpracy w sytuacjach kryzysowych pomiędzy różnymi elementami ekosystemu cybernetycznego. Takie podejście można opisać w planie działania, który powinien również zapewniać synergię i spójność z istniejącymi mechanizmami zarządzania kryzysowego[13]. Następnie należy poddać ten plan działania regularnym testom w ramach ćwiczeń w zakresie zarządzania w sytuacji kryzysu cybernetycznego lub innej sytuacji kryzysowej. W planie tym uwzględniono by rolę organów na poziomie UE, takich jak: ENISA, CERT-UE i Europejskie Centrum ds. Cyberprzestępczości (EC3) przy Europolu, a także wykorzystano by narzędzia opracowane w ramach sieci CSIRT. W pierwszej połowie 2017 r. Komisja przedstawi grupie na rzecz współpracy, sieci CSIRT i innym zainteresowanym stronom do rozpatrzenia taki plan działania w zakresie współpracy.

Wiedza, w tym wiedza ekspercka, na temat bezpieczeństwa cybernetycznego jest obecnie dostępna na poziomie unijnym, ale w sposób rozproszony i niezorganizowany. W celu wspierania mechanizmów współpracy w zakresie bezpieczeństwa sieci i informacji należy gromadzić informacje w ośrodku informacji, aby były łatwo dostępne na życzenie dla wszystkich państw członkowskich. Ten ośrodek stałby się głównym źródłem informacji umożliwiającym instytucjom UE i państwom członkowskim wymianę informacji w stosownych przypadkach. Łatwiejszy dostęp do lepiej uporządkowanych informacji na temat ryzyka dla bezpieczeństwa cybernetycznego i potencjalnych środków zaradczych powinien pomóc państwom członkowskim poszerzyć ich zdolności i dostosować praktyki, a tym samym zwiększyć ogólną odporność na ataki. Komisja – przy wsparciu ze strony ENISA i CERT-UE oraz dzięki wiedzy eksperckiej swojego Wspólnego Centrum Badawczego – ułatwi tworzenie tego ośrodka i zapewni jego stabilność.

[13] W szczególności ze zintegrowanymi uzgodnieniami dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych, w tym z decyzją w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności (z 24.07.2014) oraz procesami decyzyjnymi w dziedzinie wspólnej polityki bezpieczeństwa i obrony.

Ponadto na poziomie UE należy ustanowić regularną grupę doradczą wysokiego szczebla[14] ds. bezpieczeństwa cybernetycznego złożoną z ekspertów i decydentów z sektora przemysłu, środowiska akademickiego, społeczeństwa obywatelskiego i innych właściwych organizacji. Grupa ta umożliwiłaby Komisji pozyskiwanie w otwarty i przejrzysty sposób zewnętrznej wiedzy eksperckiej i danych wejściowych dotyczących strategii Komisji w zakresie bezpieczeństwa cybernetycznego oraz ewentualnych regulacyjnych lub innych środków z zakresu polityki publicznej. Uzupełniałaby ona inne struktury w dziedzinie bezpieczeństwa cybernetycznego[15] i byłaby z nimi połączona.

Ponadto Komisja jest zobowiązana do przeprowadzenia oceny ENISA do dnia 20 czerwca 2018 r., a ewentualna modyfikacja lub odnowienie mandatu ENISA musi nastąpić do dnia 19 czerwca 2020 r.[16]. Ze względu na obecną sytuację w dziedzinie bezpieczeństwa cybernetycznego Komisja zamierza przyspieszyć ocenę i zależnie od jej wyników jak najszybciej przedstawić wniosek dotyczący nowego mandatu.

Przy ocenie ewentualnej konieczności zmiany mandatu ENISA Komisja weźmie pod uwagę wyżej opisane wyzwania w zakresie bezpieczeństwa cybernetycznego oraz ogólne wysiłki na rzecz zacieśnienia współpracy i wymiany wiedzy. Proces ten będzie okazją do zbadania ewentualnej potrzeby zwiększenia możliwości i zdolności ENISA w zakresie trwałego wspierania państw członkowskich w osiąganiu odporności pod względem bezpieczeństwa cybernetycznego. W refleksji nad mandatem ENISA należałoby ponadto uwzględnić nowe obowiązki tej agencji w ramach dyrektywy w sprawie bezpieczeństwa sieci i informacji; nowe cele polityki odnoszące się do wspierania sektora bezpieczeństwa cybernetycznego (strategię jednolitego rynku cyfrowego, a w szczególności ustalenia umowne dotyczące partnerstwa publiczno-prywatnego); zmieniające się potrzeby w zakresie bezpieczeństwa sektorów krytycznych i nowe wyzwania związane z incydentami transgranicznymi, w tym skoordynowane reagowanie na kryzysy cybernetyczne.

Komisja:

- w pierwszej połowie 2017 r. przedłoży do rozpatrzenia plan działania w zakresie współpracy w odniesieniu do postępowania z incydentami cybernetycznymi na dużą skalę na poziomie UE;
- ułatwi utworzenie ośrodka informacji mającego na celu wspieranie wymiany informacji między organami UE i państwami członkowskimi;
- utworzy grupę doradczą wysokiego szczebla ds. bezpieczeństwa cybernetycznego oraz
- zakończy ocenę ENISA do końca 2017 r. W ocenie tej zostanie uwzględniona potrzeba modyfikacji lub rozszerzenia mandatu ENISA, co umożliwi jak najszybsze przedstawienie odnośnego wniosku.

[14] Grupy ekspertów Komisji są objęte zasadami horyzontalnymi ustanowionymi decyzja Komisji C(2016)3301.

[15] Np. platformy bezpieczeństwa sieci i informacji, partnerstwa publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego oraz platformy sektorowe, takie jak np. Platforma Ekspertów w Dziedzinie Bezpieczeństwa Cybernetycznego w Sektorze Energii. Powinna być ona również powiązana z okrągłym stołem wysokiego szczebla zapowiedzianym w komunikacie na temat cyfryzacji europejskiego przemysłu: COM(2016) 180 final.

[16] Rozporządzenie (UE) nr 526/2013 uchylające rozporządzenie (WE) nr 460/2004.

2.2 Zwiększenie wysiłków w zakresie kształcenia, szkoleń i ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego

Odpowiednie umiejętności i szkolenie, związane zarówno z zapobieganiem incydentom w sferze bezpieczeństwa cybernetycznego, jak i z postępowaniem ze skutkami tych incydentów i ich łagodzeniem, należą do kluczowych aspektów, jeżeli chodzi o osiąganie odporności pod względem bezpieczeństwa cybernetycznego.

Obecnie ENISA, europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości (ECTEG), we współpracy z Europejskim Centrum ds. Cyberprzestępczości przy Europolu, oraz Europejskie Kolegium Policyjne (CEPOL) odgrywają ważną rolę w zapewnianiu wsparcia na potrzeby budowania zdolności – w tym w dziedzinie cybernetycznej kryminalistyki – poprzez opracowywanie podręczników i organizowanie szkoleń oraz ćwiczeń dotyczących bezpieczeństwa cybernetycznego.

Cyberprzestrzeń jest jednocześnie szybko rozwijającą się dziedziną, w której zdolności podwójnego zastosowania odgrywają istotną rolę. Dlatego konieczne jest rozwijanie współpracy cywilno-wojskowej i budowanie synergii w obszarze szkoleń i ćwiczeń, aby zwiększyć odporność i zdolności UE w zakresie reagowania na incydenty.

Aby odpowiedzieć na tę potrzebę, a także w ramach działań następczych związanych z przyjęciem dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz ram polityki UE w zakresie cyberobrony[17], służby Komisji będą współpracowały z państwami członkowskimi, Europejską Służbą Działań Zewnętrznych (ESDZ), ENISA i innymi właściwymi organami UE[18] w celu ustanowienia platformy na rzecz edukacji, ćwiczeń i szkoleń w dziedzinie bezpieczeństwa cybernetycznego, której zadaniem będzie propagowania synergii między szkoleniami cywilnymi a szkoleniami obronnymi.

Komisja:

- będzie ściśle współpracowała z państwami członkowskimi, ENISA, ESDZ oraz innymi właściwymi organami UE w celu ustanowienia platformy szkoleń w dziedzinie bezpieczeństwa cybernetycznego.

2.3. Uwzględnienie współzależności międzysektorowych i odporności kluczowej publicznej infrastruktury sieciowej

Ważnym czynnikiem w ocenie ryzyka wystąpienia incydentu cybernetycznego na dużą skalę oraz skutków takiego incydentu jest stopień współzależności transgranicznych i międzysektorowych. Poważny incydent cybernetyczny w jednym sektorze lub w jednym państwie członkowskim może bezpośrednio lub pośrednio wpływać lub rozprzestrzeniać się na inne sektory lub na inne państwa członkowskie.

Współpraca transgraniczna i międzysektorowa ułatwia wymianę informacji i wiedzy eksperckiej, a tym samym osiągnięcie większej gotowości i odporności. Aby lepiej zrozumieć

[17] Przyjętymi przez Radę do Spraw Zagranicznych Unii Europejskiej w dniu 18 listopada 2014 r., dokument nr 15585/14.
[18] Takimi jak: Europejskie Kolegium Bezpieczeństwa i Obrony, EC3, CEPOL oraz Europejska Agencja Obrony (EDA).

współzależności, Komisja wspierała działania w różnych sektorach poprzez wdrożenie europejskiego programu ochrony infrastruktury krytycznej[19].

Jednocześnie koniecznym warunkiem uwzględnienia ryzyka międzysektorowego jest zdolność poszczególnych sektorów do wykrywania incydentów cybernetycznych oraz przygotowania się i reagowania na nie. Komisja oceni ryzyko wynikające z incydentów cybernetycznych w wysoce współzależnych sektorach w obrębie granic państwowych i poza nimi, w szczególności w odniesieniu do sektorów objętych dyrektywą w sprawie bezpieczeństwa sieci i informacji, również z uwzględnieniem rozwoju sytuacji na szczeblu międzynarodowym[20]. Po tej ocenie Komisja rozważy, czy istnieje potrzeba opracowania dalszych szczegółowych zasad lub wytycznych dotyczących gotowości na wypadek ryzyka cybernetycznego na potrzeby takich krytycznych sektorów.

Na szczeblu europejskim sektorowe ośrodki wymiany i analizy informacji[21] (ang. *Information Sharing and Analysis Centre,* ISAC) oraz odpowiednie CSIRT mogą odgrywać kluczową rolę w przygotowaniu się na incydenty cybernetyczne i reagowaniu na nie. W celu zapewnienia skutecznego przepływu informacji na temat zmieniających się zagrożeń oraz ułatwienia reagowania na incydenty cybernetyczne należy zachęcać ośrodki wymiany i analizy informacji do współpracy z siecią CSIRT na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz z Europejskim Centrum ds. Cyberprzestępczości przy Europolu i CERT-UE, a także właściwymi organami egzekwowania prawa.

Wymiana informacji między zainteresowanymi stronami oraz z organami podczas całego cyklu życia ryzyka cybernetycznego wymaga posiadania przez uczestników pewności, że nie narazi ich ona na odpowiedzialność. Komisja odnotowała szereg takich obaw, które powstrzymywały przedsiębiorstwa od udostępniania danych analitycznych dotyczących zagrożeń innym przedsiębiorstwom, innym sektorom lub organom, w szczególności na poziomie transgranicznym. Aby poprawić wymianę informacji na temat zagrożeń cybernetycznych, Komisja będzie dążyła do uwzględnienia i rozwiania takich obaw.

Zaufane kanały sprawozdawczości zapewniające poufność mają również kluczowe znaczenie dla zachęcania przedsiębiorstw do informowania o cyberkradzieży tajemnic przedsiębiorstwa. Umożliwiłoby to monitorowanie i ocenianie szkód poniesionych przez przemysł europejski (prowadzących także do spadku sprzedaży i utraty miejsc pracy) i instytucjom badawczym i pomogło w wypracowaniu odpowiedniej reakcji politycznej. Przy wsparciu ze strony ENISA, Urzędu Unii Europejskiej ds. Własności Intelektualnej (EUIPO) i EC3 przy Europolu Komisja utworzy – w porozumieniu z podmiotami prywatnymi – zaufane kanały do celów dobrowolnego zgłaszania cyberkradzieży tajemnic przedsiębiorstwa. Powinno to umożliwić kompilację danych przetworzonych w celu zachowania anonimowości i zagregowanych na poziomie UE. Dane te mogą być udostępniane państwom członkowskim w celu wspierania działań dyplomatycznych, jak również na potrzeby działań podnoszących świadomość, aby

[19] SWD (2013) 318.
[20] Np. planu działania w dziedzinie bezpieczeństwa cybernetycznego przyjętego przez Europejską Agencję Bezpieczeństwa Lotniczego, planu działania w dziedzinie bezpieczeństwa cybernetycznego, prac Organizacji Międzynarodowego Lotnictwa Cywilnego i Międzynarodowej Organizacji Morskiej.
[21] Zob. np. ośrodek wymiany i analizy informacji na temat europejskiego sektora energii (http://www.ee-isac.eu).

wspomóc ochronę unijnych wartości niematerialnych i prawnych przed szpiegostwem cybernetycznym.

W celu wsparcia sektorowego bezpieczeństwa cybernetycznego Komisja Europejska będzie również propagowała uwzględnianie kwestii bezpieczeństwa cybernetycznego przy opracowywaniu różnych unijnych polityk sektorowych ważnych dla tego bezpieczeństwa.

Nie mniej istotny jest fakt, że organy publiczne mają do odegrania pewną rolę, jeżeli chodzi o weryfikację integralności kluczowej infrastruktury internetowej na potrzeby wykrywania problemów, udzielanie informacji osobom odpowiedzialnym za te sieci oraz w razie potrzeby udzielanie pomocy w eliminowaniu stwierdzonych podatności na zagrożenia. Krajowe organy regulacyjne mogłyby wykorzystywać zdolności CSIRT w celu regularnego skanowania publicznej infrastruktury sieciowej i na tej podstawie zachęcać podmioty do usunięcia podatności lub luk wykrytych w ramach takiego skanowania.

W związku z tym Komisja Europejska zbada warunki prawne i organizacyjne niezbędne do umożliwienia krajowym organom regulacyjnym we współpracy z krajowymi organami ds. bezpieczeństwa cybernetycznego zwracania się do CSIRT o prowadzenie regularnych kontroli publicznej infrastruktury sieciowej pod kątem podatności na zagrożenia. Krajowe CSIRT należy zachęcać do współpracy w ramach sieci CSIRT nad najlepszymi praktykami w zakresie monitorowania sieci, co ułatwi zapobieganie incydentom na dużą skalę.

Komisja:

- będzie promowała nawiązanie współpracy na szczeblu europejskim przez sektorowe ośrodki wymiany i analizy informacji, będzie wspierała ich współpracę z CSIRT i będzie starała się wyeliminować bariery, które mogą uniemożliwiać uczestnikom rynku wymianę informacji;
- będzie badała ryzyko strategiczne/systemowe wynikające z incydentów cybernetycznych w wysoce współzależnych sektorach w obrębie granic państwowych i poza nimi;
- oceni potrzebę opracowania dodatkowych zasad lub wytycznych dotyczących gotowości na wypadek ryzyka cybernetycznego na potrzeby sektorów krytycznych i w stosownych przypadkach rozważy opracowanie takich zasad lub wytycznych;
- utworzy wraz z ENISA, EUIPO i EC3 zaufane kanały do celów dobrowolnego zgłaszania cyberkradzieży tajemnic przedsiębiorstwa;
- będzie propagowała uwzględnianie środków bezpieczeństwa cybernetycznego w europejskich politykach sektorowych oraz
- zbada warunki niezbędne do umożliwienia organom krajowym zwracania się do CSIRT o prowadzenie regularnych kontroli kluczowej infrastruktury sieciowej.

3. STAWIANIE CZOŁA WYZWANIOM STOJĄCYM PRZED JEDNOLITYM RYNKIEM BEZPIECZEŃSTWA CYBERNETYCZNEGO EUROPY

Europa potrzebuje produktów i rozwiązań w zakresie bezpieczeństwa cybernetycznego, charakteryzujących się wysoką jakością, przystępną ceną i interoperacyjnością. Podaż

produktów i usług w dziedzinie bezpieczeństwa ICT na jednolitym rynku pozostaje bardzo podzielona geograficznie. Z jednej strony utrudnia to europejskim przedsiębiorstwom konkurowanie na poziomie krajowym, europejskim i światowym, z drugiej zaś strony ogranicza wybór realnych i użytecznych technologii bezpieczeństwa cybernetycznego dostępnych dla obywateli i przedsiębiorstw[22].

Sektor bezpieczeństwa cybernetycznego w Europie rozwijał się głównie dzięki popytowi ze strony administracji krajowej, w tym na potrzeby sektora obrony. Większość europejskich wykonawców świadczących usługi na rzecz sektora obrony utworzyła duże działy ds. bezpieczeństwa cybernetycznego[23]. Równolegle powstało także mnóstwo innowacyjnych MŚP – zarówno na rynkach produktów specjalistycznych / rynkach niszowych (np. rynkach systemów kryptograficznych), jak i na ugruntowanych rynkach z nowymi modelami biznesowymi (np. rynkach programów antywirusowych).

Przedsiębiorstwa mają jednak problemy z rozszerzeniem działalności poza rynek krajowy. Brak zaufania do rozwiązań oferowanych transgranicznie jest istotnym czynnikiem, pojawiającym się często we wszystkich konsultacjach prowadzonych przez Komisję[24]. W rezultacie wiele zamówień wciąż jest udzielanych w obrębie danego państwa członkowskiego, a wiele firm ma trudności z osiągnięciem korzyści skali pozwalających im na zwiększenie swojej konkurencyjności zarówno na rynku wewnętrznym, jak i na rynku światowym.

Do luk mających wpływ na jednolity rynek bezpieczeństwa cybernetycznego należy między innymi brak interoperacyjnych rozwiązań (norm technicznych), praktyk (norm procesów) i unijnych mechanizmów certyfikacji. W związku z tym bezpieczeństwo cybernetyczne uznano za jeden z priorytetów w normalizacji ICT na jednolitym rynku cyfrowym[25].

Ograniczone perspektywy wzrostu dla przedsiębiorstw z branży bezpieczeństwa cybernetycznego na jednolitym rynku sprawiają, że dochodzi do wielu połączeń i przejęć przez inwestorów spoza Europy[26]. Chociaż tendencja ta świadczy o zdolnościach innowacyjnych europejskich przedsiębiorców w zakresie bezpieczeństwa cybernetycznego, stwarza również ryzyko doprowadzenia do utraty europejskiego know-how i wiedzy eksperckiej oraz do drenażu mózgów.

Konieczne jest pilne podjęcie działań w celu ukształtowania bardziej zintegrowanego jednolitego rynku produktów i usług z branży bezpieczeństwa cybernetycznego, który ułatwi wdrażanie praktyczniejszych i szerzej dostępnych rozwiązań.

Bariery na drodze do osiągnięcia zaufania wśród europejskich podmiotów przemysłowych i instytucjonalnych można przezwyciężyć poprzez wspieranie współpracy na wczesnym etapie cyklu życia innowacji: w samym sektorze bezpieczeństwa cybernetycznego oraz między dostawcami i nabywcami, jak również na poziomie międzysektorowym – z udziałem

[22] Zob. SWD(2016) 216.
[23] Zob. SWD(2016) 216.
[24] Zob. SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Zob. SWD(2016) 216.

sektorów, które już są lub mogą stać się nabywcami rozwiązań w zakresie bezpieczeństwa cybernetycznego.

Jednocześnie rozwój produktów, usług i technologii podwójnego zastosowania staje się coraz ważniejszy w Europie. Na rynek obronności trafia coraz więcej rozwiązań z rynku cywilnego[27]. W przyszłym europejskim planie działań w sektorze obrony Komisja zamierza określić środki na rzecz dalszego zwiększenia cywilno-wojskowego efektu synergii na poziomie europejskim.

3.1 Certyfikacja i oznakowanie

Certyfikacja odgrywa ważną rolę we wzmacnianiu zaufania do produktów i usług oraz w zwiększaniu ich bezpieczeństwa. Odnosi się to również do tych nowych systemów, w których intensywnie wykorzystuje się technologie cyfrowe, które wymagają wysokiego poziomu bezpieczeństwa, takich jak: systemy stosowane w samochodach automatycznych połączonych z systemami informatycznymi czy w sektorze e-zdrowia, przemysłowe systemy automatycznego sterowania lub inteligentne sieci energetyczne.

Pojawiają się krajowe inicjatywy na rzecz ustanowienia wymogów zapewniających wysoki poziom bezpieczeństwa cybernetycznego elementów ICT w infrastrukturze tradycyjnej, w tym wymogów w zakresie certyfikacji. Choć wymogi te są ważne, stwarzają ryzyko fragmentacji jednolitego rynku i pojawienia się problemów dotyczących interoperacyjności. Tylko w kilku państwach członkowskich istnieją skuteczne systemy certyfikacji bezpieczeństwa produktów ICT[28]. Dostawca produktów ICT może zatem być zmuszony do przejścia kilku procesów certyfikacji, aby móc sprzedawać swoje produkty w kilku państwach członkowskich. W najgorszym wypadku produkty lub usługi informatyczne zaprojektowane w celu spełnienia wymogów bezpieczeństwa cybernetycznego w jednym państwie członkowskim nie będą mogły być wprowadzone do obrotu w innym państwie.

Aby osiągnąć funkcjonujący jednolity rynek w dziedzinie bezpieczeństwa cybernetycznego ramy certyfikacji bezpieczeństwa cybernetycznego produktów i usług ICT powinny zmierzać do zrealizowania następujących celów: (i) objęcia tymi ramami szerokiej gamy systemów, produktów i usług ICT; (ii) zapewnienia, aby ramy te miały zastosowanie do wszystkich 28 państw członkowskich oraz (iii) uwzględnienia wszystkich poziomów bezpieczeństwa cybernetycznego, biorąc pod uwagę rozwój sytuacji na szczeblu międzynarodowym.

W ty celu Komisja powoła specjalną grupę roboczą ds. certyfikacji bezpieczeństwa produktów i usług ICT, w której skład wejdą eksperci z państw członkowskich i branży. Jej zadaniem będzie opracowanie do końca 2016 r., we współpracy z ENISA i Wspólnym Centrum Badawczym, planu działania, w którym zbadane zostaną możliwości stworzenia takich europejskich ram certyfikacji bezpieczeństwa ICT, który to wniosek zostałby złożony przed końcem 2017 r. W związku z tym Komisja uwzględni również rozporządzenie (WE)

[27] W 2013 r. wywóz produktów podwójnego zastosowania stanowił już około 20 % całkowitego wywozu UE (pod względem wartości). Obejmuje to handel wewnątrz UE.

[28] W kwestii porozumienia grupy urzędników wysokiego szczebla ds. systemów informacyjnych (decyzja Rady z dnia 31 marca 1992 r. (92/242/EWG)) oraz inne istniejące systemy, np. Commercial Product Assurance w Zjednoczonym Królestwie i Certification Sécuritaire de Premier Niveau we Francji, zob. SWD(2016) 216.

nr 2008/765 i przepisy dotyczące certyfikacji zawarte w ogólnym rozporządzeniu o ochronie danych (UE) 2016/679[29].

Proces ten będzie obejmował szeroko zakrojone konsultacje i ocenę skutków. Umożliwi to Komisji przeanalizowanie różnych wariantów utworzenia ram certyfikacji produktów i usług ICT. Komisja zbada również możliwość uwzględnienia poświadczania bezpieczeństwa cybernetycznego ICT w sektorach infrastruktury (np. w odniesieniu do sektorów lotnictwa, kolejowego lub motoryzacyjnego) oraz w ramach konkretnych mechanizmów certyfikacji i walidacji gotowych do wdrożenia technologii (np. bezpieczeństwa cybernetycznego przemysłowych systemów automatycznego sterowania[30], internetu rzeczy, chmury). Rozwiąże to też kwestię likwidacji stwierdzonych luk w obrębie wyżej wspomnianego europejskiego systemu certyfikacji bezpieczeństwa ICT.

Jak najwięcej działań dotyczących certyfikacji, które zostaną opracowane we współpracy z partnerami międzynarodowymi, będzie opartych na uznanych normach międzynarodowych.

Komisja przeanalizuje również sposoby jak najlepszego uwzględnienia certyfikacji bezpieczeństwa ICT w przyszłych przepisach sektorowych, także związanych z aspektami bezpieczeństwa.

Oprócz możliwych wariantów regulacyjnych Komisja zbada również możliwość utworzenia europejskiego systemu oznakowania dotyczącego bezpieczeństwa produktów ICT, który byłby ukierunkowany komercyjnie, dobrowolny i związany z niewielkim obciążeniem dla uczestniczących w nim podmiotów. Będzie on stanowił uzupełnienie certyfikacji i służył poprawieniu czytelności oznakowania dotyczącego bezpieczeństwa cybernetycznego produktów komercyjnych, aby zwiększyć ich konkurencyjność na jednolitym rynku i na całym świecie. Aktualne inicjatywy sektorowe i horyzontalne podejmowane przez branżę, zarówno po stronie podaży, jak i po stronie popytu, zostaną należycie uwzględnione.

Administracja publiczna zostanie ściśle zaangażowana we współpracę, aby umożliwić stosowanie wspólnych specyfikacji i odniesień do certyfikacji przy udzielaniu zamówień publicznych. Komisja będzie również monitorowała stosowanie odpowiednich wymogów w zakresie certyfikacji w udzielaniu zamówień publicznych na poziomie krajowym, w szczególności w systemach sektorowych (w sektorach energii, transportu, zdrowia, administracji publicznej itp.), oraz przedstawi sprawozdanie na ten temat.

Komisja:

- do końca 2016 r. opracuje plan działania prowadzący do sformułowania wniosku w sprawie ewentualnych europejskich ram certyfikacji bezpieczeństwa ICT, który to wniosek zostałby złożony przed końcem 2017 r., oraz przeprowadzi ocenę wykonalności i skutków europejskich ram oznakowania dotyczącego

[29] W rozporządzeniu Parlamentu Europejskiego i (EU) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, określono zarówno kodeks postepowania mający na celu przyczynienie się do właściwego stosowania przepisów dotyczących ochrony danych, jak również mechanizmów certyfikacji, obejmujących wszystkie zasady ochrony danych, w tym zwłaszcza bezpieczeństwo przetwarzania danych osobowych.

[30] Zob. grupa tematyczna w sprawie bezpieczeństwa cybernetycznego przemysłowych systemów kontroli: https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems

bezpieczeństwa charakteryzujących się niewielkim obciążeniem dla uczestniczących w nich podmiotów;
- przeanalizuje potrzebę zlikwidowania luk pod względem certyfikacji bezpieczeństwa ICT obecnych w istniejących mechanizmach certyfikacji/walidacji dotyczących określonych sektorów oraz w stosownych przypadkach wyeliminuje te luki;
- włączy, w stosownych przypadkach, certyfikację bezpieczeństwa produktów ICT do przyszłych unijnych wniosków prawodawczych;
- będzie pobudzała zaangażowanie administracji publicznej, aby ułatwić stosowanie certyfikacji i wspólnych specyfikacji przy udzielaniu zamówień publicznych oraz
- będzie monitorowała stosowanie odpowiednich wymogów w zakresie certyfikacji w udzielaniu zamówień publicznych i prywatnych oraz po trzech latach przedstawi sprawozdanie na temat stanu rynku.

3.2. Zwiększanie skali inwestycji w dziedzinie bezpieczeństwa cybernetycznego w Europie i wsparcia dla MŚP

Chociaż sektor bezpieczeństwa cybernetycznego w Europie charakteryzuje się znaczną innowacyjnością, Unia Europejska nadal nie ma odpowiedniej kultury inwestowania w bezpieczeństwo cybernetyczne. Istnieje wiele innowacyjnych MŚP w tej dziedzinie, ale często nie są one w stanie zwiększyć skali swojej działalności. Jedną z przyczyn jest brak łatwo dostępnego finansowania, które stanowiłoby wsparcie na wczesnych etapach rozwoju. Przedsiębiorstwa mają również ograniczony dostęp do kapitału wysokiego ryzyka w Europie, a dostępny budżet na marketing, który by poprawił ich widoczność lub umożliwił poradzenie sobie z różnymi zbiorami wymogów dotyczących normalizacji i zgodności, jest niewystarczający.

Jednocześnie współpraca między różnymi podmiotami w sektorze bezpieczeństwa cybernetycznego jest bardzo nierówna i potrzebne są dalsze działania w celu zwiększenia koncentracji gospodarczej i utworzenia nowych łańcuchów wartości[31].

Aby zwiększyć skalę inwestycji w dziedzinie bezpieczeństwa cybernetycznego w Europie i wsparcia dla MŚP, konieczne jest ułatwienie dostępu do finansowania. Niezbędne jest również wsparcie dla rozwoju globalnie konkurencyjnych klastrów bezpieczeństwa cybernetycznego i centrów doskonałości w ekosystemach regionalnych sprzyjających wzrostowi cyfrowemu. Wsparcie to musi być związane z realizacją strategii inteligentnej specjalizacji i innych instrumentów UE, tak aby sektor bezpieczeństwa cybernetycznego w Europie lepiej z nich korzystał.

Podejście Komisji będzie polegało na maksymalnym zwiększeniu wiedzy społeczności zajmującej się bezpieczeństwem cybernetycznym na temat możliwości uzyskania finansowania na poziomie europejskim, krajowym i regionalnym (w odniesieniu zarówno do

[31] Zob. SWD(2016) 216.

instrumentów horyzontalnych, jak i konkretnych zaproszeń do składania wniosków[32]) za pomocą istniejących instrumentów i kanałów, np. Europejskiej Sieci Przedsiębiorczości.

Komisja będzie uzupełniała te działania, analizują wspólnie z Europejskim Bankiem Inwestycyjnym (EBI) i Europejskim Funduszem Inwestycyjnym (EIF) sposoby ułatwienia dostępu do finansowania. Może to nastąpić w postaci pożyczek na inwestycje kapitałowe i quasi-kapitałowe, kredytów i gwarancji[33] na projekty lub kontrgwarancji dla podmiotów pośredniczących, np. poprzez utworzenie specjalnej platformy inwestycyjnej w dziedzinie bezpieczeństwa cybernetycznego w ramach Europejskiego Funduszu na rzecz Inwestycji Strategicznych (EFIS)[34]

Ponadto Komisja rozważy również utworzenie wraz z zainteresowanymi regionami i państwami członkowskimi platformy inteligentnej specjalizacji w dziedzinie bezpieczeństwa cybernetycznego[35], której zadaniem byłoby koordynowanie i planowanie realizacji strategii w zakresie bezpieczeństwa cybernetycznego oraz organizowanie strategicznej współpracy podmiotów w ekosystemach regionalnych. Podejście to powinno również pomóc uwolnić potencjał istniejących europejskich funduszy strukturalnych i inwestycyjnych w odniesieniu do sektora bezpieczeństwa cybernetycznego.

W bardziej ogólnym ujęciu Komisja będzie propagowała podejście oparte na uwzględnianiu bezpieczeństwa na etapie projektowania i dążyła do zapewnienia, aby wymogi w zakresie bezpieczeństwa cybernetycznego były konsekwentnie uwzględniane we wszystkich poważnych inwestycjach w infrastrukturę, które mają element cyfrowy i są współfinansowane z funduszy europejskich, poprzez stopniowe wprowadzanie odpowiednich wymogów do zasad udzielania zamówień oraz do zasad programów.

Komisja:

- będzie stosowała istniejące narzędzia wsparcia MŚP w celu poszerzenia wiedzy społeczności zajmującej się bezpieczeństwem cybernetycznym na temat istniejących mechanizmów finansowania;
- jeszcze bardziej zintensyfikuje wykorzystanie unijnych narzędzi i instrumentów do wspierania innowacyjnych MŚP w badaniu synergii między rynkiem cywilnym a rynkiem obronnym w zakresie bezpieczeństwa cybernetycznego[36];
- zbada wraz z EBI i EFI możliwość ułatwienia dostępu do inwestycji np. za pośrednictwem specjalnej platformy inwestycyjnej w dziedzinie bezpieczeństwa cybernetycznego lub za pomocą innych narzędzi;
- utworzy platformę inteligentnej specjalizacji w dziedzinie bezpieczeństwa cybernetycznego, aby pomóc państwom i regionom zainteresowanym

[32]. Zob. np. wielosektorowe zaproszenie do składania wniosków z 2016 r. w ramach instrumentu „Łącząc Europę” oraz zaproszenia w ramach COSMO z 2016 r. związane z Programem Internacjonalizacji Klastrów.

[33] W ramach Europejskiego Funduszu Inwestycji Strategicznych indywidualne projekty mogą być wspierane albo bezpośrednio albo pośrednio poprzez platformy inwestycyjne. Takie platformy mogą pomóc w finansowaniu mniejszych projektów i skupiać fundusze z różnych źródeł na potrzeby zróżnicowanych inwestycji ukierunkowanych geograficznie bądź tematycznie.

[34] Zob. instrumenty inteligentnej specjalizacji (RIS3): http://s3platform.jrc.ec.europa.eu/

[35] Na przykład Europejska Sieć Przedsiębiorczości i europejska sieć regionów związanych z obronnością zapewnią regionom nowe możliwości współpracy transgranicznej w dziedzinie produktów podwójnego zastosowania, w tym bezpieczeństwa cybernetycznego, a MŚP – nowe możliwości prowadzenia działalności w zakresie kojarzenia partnerów biznesowych.

[36]. Partnerstwo publiczno-prywatne „Infrastruktura 5G” oraz partnerstwo publiczno-prywatne „Duże zbiory danych”.

inwestowaniem w sektorze bezpieczeństwa cybernetycznego (RIS3) oraz
- będzie propagowała stosowanie podejścia opartego na uwzględnianiu bezpieczeństwa na etapie projektowania we wszystkich poważnych inwestycjach w infrastrukturę, które zawierają element cyfrowy i są współfinansowane z funduszy unijnych.

4. POBUDZANIE I WSPIERANIE ROZWOJU EUROPEJSKIEJ BRANŻY BEZPIECZEŃSTWA CYBERNETYCZNEGO POPRZEZ INNOWACJĘ – UTWORZENIE KONTRAKTOWEGO PARTNERSTWA PUBLICZNO-PRYWATNEGO

Aby pobudzać konkurencyjność i innowacyjność europejskiego sektora bezpieczeństwa cybernetycznego, powołane zostanie kontraktowe partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego. Kontraktowe partnerstwo publiczno-prywatne pozwoli zgromadzić zasoby branżowe i publiczne, aby osiągnąć doskonałość w zakresie badań naukowych i innowacji.

Celem kontraktowego partnerstwa publiczno-prywatnego jest budowanie zaufania pomiędzy państwami członkowskimi i podmiotami branżowymi poprzez wspieranie współpracy na wczesnych etapach procesu badawczo-innowacyjnego. Ma ono na celu również wspomaganie dostosowania sektorów popytu i podaży. Powinno to umożliwić branży uzyskanie wiedzy na temat przyszłych wymagań ze strony użytkowników końcowych, a także sektorów, które są ważnymi nabywcami rozwiązań w zakresie bezpieczeństwa cybernetycznego (np. sektory energii, zdrowia, transportu, finansów). Ułatwi to zaangażowanie tych podmiotów w formułowanie wspólnych wymogów w zakresie bezpieczeństwa cyfrowego oraz ochrony prywatności i danych w ich sektorach.

Kontraktowe partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego pozwoli również zmaksymalizować wykorzystanie dostępnych środków finansowych. Cel ten zostanie zrealizowany po pierwsze poprzez lepszą koordynację z państwami członkowskimi. Po drugie, możliwe będzie skupienie się w większym stopniu na kilku priorytetach technicznych, aby pomóc sektorowi bezpieczeństwa cybernetycznego w dokonaniu przełomów technologicznych i opanowaniu kluczowych przyszłych technologii bezpieczeństwa cybernetycznego. W tym kontekście tworzenie otwartego oprogramowania i otwartych standardów może sprzyjać budowaniu zaufania i przejrzystości oraz innowacjom radykalnym, w związku z czym będzie również stanowić część inwestycji w ramach tego kontraktowego partnerstwa publiczno-prywatnego.

Prace prowadzone w ramach kontraktowego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego wykorzystają również efekt synergii z innymi europejskimi projektami, w szczególności tymi, które dotyczą aspektów bezpieczeństwa, takich jak aspekty obecne w partnerstwach publiczno-prywatnych dotyczących fabryk jutra, energooszczędnych budynków, infrastruktury sieci 5G oraz dużych zbiorów danych[37], a także w innych sektorowych partnerstwach publiczno-prywatnych[38] oraz w inicjatywie dotyczącej internetu

[37]. Na przykład w partnerstwie publiczno-prywatnym SESAR lub Shift2Rail.
[38]. Sojusz na rzecz innowacji w dziedzinie internetu rzeczy (ang. *Alliance for Internet of Things Innovation*, AIOTI).

rzeczy[39]. Ponadto promowane będzie zharmonizowanie działań z europejską chmurą dla otwartej nauki oraz z europejską inicjatywą na rzecz kwantowych cybernetycznych technologii komputerowych dużej wydajności (np. innowacji w zakresie kwantowej dystrybucji klucza, badań nad kwantowymi technologiami obliczeniowymi).

Kontraktowe partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego powstaje w ramach „Horyzontu 2020" – programu ramowego UE w zakresie badań naukowych i innowacji na lata 2014-2020. Pobudzi ono finansowanie z dwóch filarów tego programu: „Wiodąca pozycja w zakresie technologii prorozwojowych i przemysłowych" oraz 7. celu szczegółowego „Bezpieczne społeczeństwa" w obrębie priorytetu „Wyzwania społeczne". Całkowity budżet kontraktowego partnerstwa publiczno-prywatnego wyniesie do 450 mln EUR przy potrójnej dźwigni finansowej po stronie sektora. Bezpieczeństwem cybernetycznym należy także zajmować się w sposób skoordynowany z innymi istotnymi częściami programu „Horyzont 2020" (np. dotyczącymi wyzwań społecznych w zakresie energii, transportu i zdrowia oraz doskonałości). Przyczyni się to do realizacji celów kontraktowego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego. Koordynacja ta powinna również poprzedzać etap formułowania strategii sektorowych.

Kontraktowe partnerstwo publiczno-prywatne zostanie wdrożone w sposób przejrzysty, w oparciu o otwarte i elastyczne zarządzanie dostosowane do szybko zmieniającego się środowiska bezpieczeństwa cybernetycznego. Zostanie przy tym również uwzględniona konieczność omówienia przez państwa członkowskie wpływu zmian technologii na bezpieczne funkcjonowanie infrastruktury krajowej i transgranicznej. Jednocześnie skutek partnerstwa musi być trwały przez kilka lat w celu zagwarantowania, że jego cele zostały zrealizowane

Kontraktowe partnerstwo publiczno-prywatne będzie wspierane przez Europejską Organizację na rzecz Bezpieczeństwa Cybernetycznego (ang. *European Cyber Security Organisation*, ECSO), w której skład – odzwierciedlający różnorodność rynku bezpieczeństwa cybernetycznego w Europie. Obejmie ono krajowe, regionalne i lokalne administracje publiczne, ośrodki badań naukowych, a także inne zainteresowane strony.

Komisja:

- zawrze z branżą kontraktowe partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego, tak aby rozpoczęło ono działalność w trzecim kwartale 2016 r.;
- w pierwszym kwartale 2017 r. w ramach programu „Horyzont 2020" opublikuje zaproszenia do składania wniosków w ramach kontraktowego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego oraz
- zapewni koordynację kontraktowego partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego ze stosownymi strategiami sektorowymi, instrumentami programu „Horyzont 2020" i sektorowymi partnerstwami publiczno-

[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents

prywatnymi.

5. PODSUMOWANIE

W niniejszym komunikacie przedstawiono środki mające na celu wzmocnienie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego w Europie, jak zapowiedziano w unijnej strategii w zakresie bezpieczeństwa cybernetycznego oraz w strategii jednolitego rynku cyfrowego. Komisja zwraca się do Parlamentu Europejskiego i Rady o poparcie przyjętego podejścia.