KOMISJA
EUROPEJSKA

WYSOKI PRZEDSTAWICIEL UNII
DO SPRAW ZAGRANICZNYCH I
POLITYKI BEZPIECZEŃSTWA

Bruksela, dnia 13.9.2017 r.
JOIN(2017) 450 final

WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY

Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej

1. WPROWADZENIE

Bezpieczeństwo cybernetyczne ma kluczowe znaczenie zarówno dla naszego dobrobytu, jak również dla naszego bezpieczeństwa. W miarę wzrostu poziomu uzależnienia naszego codziennego życia i gospodarki od technologii cyfrowych stopień naszego narażenia na zagrożenia rośnie. Incydenty cybernetyczne stają się coraz bardziej zróżnicowane, zarówno pod względem tego, kto jest za nie odpowiedzialny, jak i celów, jakie chcą osiągnąć ich sprawcy. Szkodliwe działania cybernetyczne stanowią zagrożenie nie tylko dla naszych gospodarek i dążenia do jednolitego rynku cyfrowego, ale także dla samego funkcjonowania naszych demokracji, dla naszych wolności i naszych wartości. Nasze bezpieczeństwo w przyszłości zależy od naszej zdolności do ochrony UE przed zagrożeniami cybernetycznymi: zarówno infrastruktura cywilna, jak potencjał wojskowy są zależne od bezpiecznych systemów cyfrowych. Uznano to na posiedzeniu Rady Europejskiej w czerwcu 2017 r.[1], a także zapisano w globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej[2].

Ryzyko to rośnie lawinowo. Z badań wynika, że gospodarcze skutki zjawiska cyberprzestępczości wzrosły pięciokrotnie w latach 2013–2017, a do 2019 r. mogą ponownie wzrosnąć czterokrotnie[3]. Odnotowano szczególny wzrost oprogramowania szantażującego (ang. *ransomware*)[4], a najnowsze ataki[5] odzwierciedlają gwałtowną intensyfikację przestępczej działalności cybernetycznej. Oprogramowanie szantażujące nie jest jednak jedynym zagrożeniem.

Źródłami zagrożeń cybernetycznych są zarówno podmioty niepaństwowe, jak i państwowe: często zagrożenia te mają charakter przestępczy i wynikają z chęci zysku, ale mogą być także warunkowane politycznie lub strategicznie. Zagrożenie przestępcze ulega wzmocnieniu wskutek zacierania się granic między cyberprzestępczością a tradycyjną przestępczością, gdyż przestępcy wykorzystują internet zarówno jako sposób rozszerzania swojej działalności, jak również jako źródło nowych metod i narzędzi do popełniania przestępstw[6]. W znacznej większości przypadków szanse wytropienia przestępcy są minimalne, a szanse pociągnięcia go do odpowiedzialności – jeszcze mniejsze.

Jednocześnie podmioty państwowe w coraz większym stopniu realizują swoje cele geopolityczne nie tylko za pomocą tradycyjnych narzędzi, takich jak siły zbrojne, ale również dzięki dyskretniejszym w użyciu narzędziom cybernetycznym, obejmującym wpływanie na wewnętrzne procesy demokratyczne. Wykorzystywanie cyberprzestrzeni jako obszaru prowadzenia wojny, autonomicznie lub w ramach podejścia hybrydowego, jest obecnie powszechnie znanym faktem. Kampanie dezinformacyjne, rozpowszechnianie fałszywych informacji oraz operacje cybernetyczne nakierowane na infrastrukturę krytyczną są coraz bardziej powszechne i wymagają reakcji. Z tego względu w dokumencie otwierającym debatę

---

1 http://www.consilium.europa.eu/pl/press/press-releases/2017/06/23-euco-conclusions/

2 http://europa.eu/globalstrategy/.

3 Przykłady: zob. McAfee & Centre for Strategic and International Studies, *Net losses: Estimating the Global Cost of Cybercrime* (Straty netto: oszacowanie globalnych kosztów cyberprzestępczości) 2014.

4 Oprogramowanie szantażujące jest rodzajem złośliwego oprogramowania, które utrudnia lub ogranicza użytkownikom dostęp do ich systemu przez zablokowanie ekranu systemu lub plików użytkownika do momentu wpłacenia okupu.

5 W maju 2017 r. atak oprogramowania szantażującego WannaCry dotknął ponad 400 000 komputerów w ponad 150 krajach. Miesiąc później atak z użyciem oprogramowania Petya dotknął Ukrainę i kilka przedsiębiorstw na całym świecie.

6 Przedłożona przez Europol Ocena zagrożenia poważną i zorganizowaną przestępczością, 2017.

na temat przyszłości europejskiej obronności[7] Komisja podkreśliła znaczenie współpracy w zakresie obrony cybernetycznej.

Jeżeli znacząco nie poprawimy poziomu naszego bezpieczeństwa cybernetycznego, ryzyko będzie wzrastać w miarę postępów transformacji cyfrowej. Oczekuje się, że do 2020 r. do internetu podłączonych będzie kilkadziesiąt miliardów obiektów w „internecie rzeczy", ale bezpieczeństwo cyfrowe nie zyskało jeszcze priorytetu w ich projektowaniu[8]. Brak zapewnienia ochrony urządzeń, które będą kontrolować nasze sieci energetyczne, samochody i sieci transportowe, zakłady przemysłowe, sferę finansową, szpitale i domy, może mieć katastrofalne skutki i znacznie nadwerężyć zaufanie konsumentów do powstających technologii. Ryzyko motywowanych politycznie ataków na cele cywilne i niesprawności militarnej obrony cybernetycznej dodatkowo wzmacniają stopień zagrożenia.

Podejście określone w niniejszym wspólnym komunikacie poprawi pozycję UE w obliczu tych zagrożeń. Będzie ono podstawą większej odporności i strategicznej autonomii, wzmocni zdolności w zakresie technologii i umiejętności oraz pomoże w budowie silnego jednolitego rynku. Wymaga to posiadania właściwych struktur w celu zbudowania solidnego bezpieczeństwa cybernetycznego i reagowania w razie potrzeby, z pełnym zaangażowaniem wszystkich kluczowych podmiotów. Podejście to umożliwiłoby też lepsze zapobieganie atakom cybernetycznym przez wzmocnienie działań w celu wykrywania, śledzenia i pociągania winnych do odpowiedzialności. Uwzględniony zostanie też wymiar globalny dzięki rozwijaniu współpracy międzynarodowej jako platformy dla przewodniej roli UE w dziedzinie bezpieczeństwa cybernetycznego. Działania te wynikają z podejścia określonego w ramach jednolitego rynku cyfrowego, globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej, europejskiej agendy bezpieczeństwa[9], wspólnych ram przeciwdziałania zagrożeniom hybrydowym[10] oraz z komunikatu na temat utworzenia Europejskiego Funduszu Obronnego[11][12].

UE zajmuje się już wieloma z tych kwestii: obecnie nadszedł czas zespolenia tych różnych wysiłków. W 2013 r. UE sformułowała strategię bezpieczeństwa cybernetycznego, w której wytyczono wiele kierunków działań, prowadzących do zwiększenia odporności na zagrożenia cybernetyczne[13]. Jej główne cele i zasady, polegające na zapewnieniu niezawodnego, bezpiecznego i otwartego środowiska cybernetycznego, zachowują aktualność. Wciąż zmieniające się i rosnące zagrożenia zmuszają jednak do intensywniejszych działań w celu stawienia oporu i zapobieżenia przyszłym atakom[14].

UE jest dobrze przygotowana do zajęcia się kwestiami bezpieczeństwa cybernetycznego z uwagi na zakres swoich polityk i narzędzi oraz struktury i zdolności, jakimi dysponuje. Państwa członkowskie pozostają odpowiedzialne za swoje bezpieczeństwo narodowe, skala

---

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_pl.pdf

8 IDC and TXT Solutions (2014), SMART 2013/0037 *Cloud and IoT combination* (Połączenie chmury i internetu rzeczy), badanie przeprowadzone na zlecenie Komisji Europejskiej.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Podejście to zostało również potwierdzone w niezależnej opinii naukowej przedłożonej przez powołaną przez Komisję grupę wysokiego szczebla doradców naukowych ds. mechanizmów doradztwa naukowego (zob. odesłania poniżej).

13 JOIN(2013) 1 final. Ocena tej strategii jest dostępna w dokumencie roboczym SWD(2017) 295.

14 Jeżeli nie zaznaczono inaczej, propozycje zawarte w niniejszym komunikacie nie mają wpływu na budżet. Każda inicjatywa mająca wpływ na budżet podlega stosownym dorocznym procedurom budżetowym i nie może naruszać kolejnych wieloletnich ram finansowania na lata po 2020 r.

i transgraniczny charakter zagrożeń w znaczący sposób uzasadniają jednak podejmowanie przez UE działań zachęcających państwa członkowskie do budowy i utrzymywania większego i lepszego potencjału w zakresie bezpieczeństwa cybernetycznego oraz wspierających państwa członkowskie w tych wysiłkach, przy jednoczesnym budowaniu zdolności na szczeblu unijnym. Podejście takie ma na celu pobudzenie wszystkich podmiotów – UE, państw członkowskich, przemysłu i osób fizycznych – do nadania bezpieczeństwu cybernetycznemu priorytetu potrzebnego do budowania odporności i zapewnienia lepszej reakcji UE na ataki cybernetyczne. Przyniesie ono konkretne działania pomocne w wykrywaniu i prowadzeniu dochodzeń w przypadku wszelkich incydentów cybernetycznych przeciwko UE oraz jej państwom członkowskim, a także służące do odpowiedniego reagowania, łącznie ze ściganiem przestępców. Umożliwi to skuteczne wspieranie bezpieczeństwa cybernetycznego na arenie międzynarodowej za pośrednictwem działań zewnętrznych UE. Rezultatem będzie zmiana unijnego podejścia z reagowania na zagrożenia na ich aktywne przewidywanie i zapobieganie im obecnie i w przyszłości w celu ochrony dobrobytu, społeczeństwa i wartości europejskich, a także podstawowych praw i wolności.

2. BUDOWANIE ODPORNOŚCI UE NA ATAKI CYBERNETYCZNE

Duża odporność cybernetyczna wymaga wspólnego i szeroko zakrojonego podejścia. Potrzebne są silniejsze i skuteczniejsze struktury na potrzeby zapewnienia bezpieczeństwa cybernetycznego i reagowania na ataki cybernetyczne w państwach członkowskich, ale także we własnych instytucjach UE, jej agencjach i organach. Budowanie takiej odporności wymaga również przyjęcia bardziej kompleksowego podejścia, w ujęciu przekrojowym w stosunku do unijnych polityk, do kształtowania odporności na zagrożenia cybernetyczne oraz strategicznej autonomii, z silnym jednolitym rynkiem. znacznych postępów w zakresie zdolności technologicznych UE oraz znacznie większej liczby wykwalifikowanych specjalistów. Kwestią centralną jest szersza akceptacja bezpieczeństwa cybernetycznego jako wspólnego wyzwania społecznego, tak aby możliwe było zaangażowanie różnych szczebli administracji rządowej, sfery gospodarczej i społeczeństwa.

2.1 Wzmocnienie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) ma do odegrania kluczową rolę we wzmocnieniu odporności UE na zagrożenia cybernetyczne i reagowaniu na nie, ale jest ograniczona swoim obecnym mandatem. Dlatego Komisja przedstawia ambitną propozycję reformy, która obejmuje między innymi **stały mandat tej agencji**[15]. Zagwarantuje to możliwość zapewniania przez ENISA wsparcia dla państw członkowskich, instytucji UE i przedsiębiorstw w kluczowych dziedzinach, w tym we wdrażaniu dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych[16] („dyrektywy w sprawie bezpieczeństwa sieci i informacji") oraz proponowanych ram certyfikacji bezpieczeństwa cybernetycznego.

[15] COM(2017) 477.

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Zreformowana ENISA odegra silną rolę doradczą w kwestii opracowywania i realizacji działań, łącznie ze wspieraniem spójności między inicjatywami sektorowymi i dyrektywą w sprawie bezpieczeństwa sieci i systemów informatycznych oraz wspomaganiem powoływania ośrodków wymiany i analizy informacji w sektorach o kluczowym znaczeniu. ENISA podniesie poziom europejskiej gotowości i wzmocni ją dzięki organizowaniu dorocznych ogólnoeuropejskich ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego, łączących reagowanie na różnych poziomach. Agencja wesprze również opracowanie polityki UE w zakresie certyfikacji bezpieczeństwa cybernetycznego technologii informacyjno-komunikacyjnych (ICT) oraz odegra ważną rolę w zacieśnianiu współpracy operacyjnej i zarządzania kryzysowego w obrębie UE. Będzie również służyć jako centrum informacji i wiedzy w społeczności zajmującej się bezpieczeństwem cybernetycznym.

Szybkie i wspólne zrozumienie zagrożeń i incydentów w miarę ich pojawiania się jest warunkiem koniecznym do podjęcia decyzji co do potrzeby wspólnego ograniczania skutków lub reagowania wspieranego przez UE. Taka wymiana informacji wymaga zaangażowania wszystkich odnośnych podmiotów – organów i agencji UE, a także państw członkowskich – na poziomie technicznym, operacyjnym i strategicznym. ENISA we współpracy z odpowiednimi organami na szczeblu państw członkowskich i UE, zwłaszcza siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego[17], CERT-UE, Europolem i Centrum Analiz Wywiadowczych UE (INTCEN), przyczyni się także do orientacji sytuacyjnej na szczeblu unijnym. Zostanie to włączone do działań wywiadowczych w zakresie zagrożeń oraz kształtowania polityki w ramach regularnego monitorowania zagrożeń i skutecznej współpracy operacyjnej, a także do reagowania na incydenty transgraniczne na dużą skalę.

2.2 W kierunku jednolitego rynku bezpieczeństwa cybernetycznego

Rozwój rynku bezpieczeństwa cybernetycznego w UE – w zakresie produktów, usług i procesów – został pod wieloma względami zahamowany. Kluczowym aspektem jest brak systemów certyfikacji bezpieczeństwa cybernetycznego uznawanych w całej UE, służących do wyposażania produktów w wyższe standardy odporności oraz budowania podstaw ogólnounijnego zaufania rynku. Dlatego Komisja występuje z wnioskiem o ustanowienie **ram certyfikacji bezpieczeństwa cybernetycznego UE**[18]. W ramach tych określono by procedurę tworzenia ogólnounijnych systemów certyfikacji bezpieczeństwa cybernetycznego, obejmujących produkty, usługi i systemy, które dostosowują poziom bezpieczeństwa do odpowiedniego sposobu wykorzystania (czy to w przypadku infrastruktury krytycznej, czy urządzeń konsumenckich)[19]. Przyniosłoby to wyraźne korzyści przedsiębiorstwom poprzez wyeliminowanie konieczności poddawania się kilku procesom certyfikacji w handlu transgranicznym i w ten sposób ograniczyłoby koszty administracyjne i obciążenia finansowe. Zastosowanie systemów opracowanych na podstawie tych zasad ramowych pomogłoby również budować zaufanie konsumentów: świadectwo zgodności informowałoby i upewniało nabywców i użytkowników co do właściwości w zakresie bezpieczeństwa produktów i usług, które nabywają i z których korzystają. Dzięki temu wysokie standardy w zakresie bezpieczeństwa cybernetycznego stałyby się źródłem przewagi konkurencyjnej. Rezultatem byłoby wzmocnienie odporności, gdyż produkty i usługi ICT byłyby formalnie oceniane pod

[17] Określoną w art. 9 dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych.

[18] COM(2017) 477.

[19] Poziom bezpieczeństwa wskazuje stopień dokładności oceny bezpieczeństwa i zwykle jest współmierny do poziomu ryzyka związanego z danymi obszarami zastosowania bądź funkcjami (tj. wyższego poziomu bezpieczeństwa wymaga się od produktów i usług ICT stosowanych w obszarach zastosowań lub funkcji wysokiego ryzyka).

kątem ustalonego zestawu norm dotyczących bezpieczeństwa cybernetycznego, które to normy mogłyby zostać opracowane w ścisłym powiązaniu z szerszym zakresem prowadzonych obecnie prac nad normami ICT[20].

Przyjęcie systemów zgodnych z ramami byłoby dobrowolne i nie spowodowałoby żadnych natychmiastowych zobowiązań prawnych po stronie sprzedawców lub dostawców usług. Systemy nie byłyby sprzeczne z żadnymi obowiązującymi wymogami prawnymi, takimi jak przepisy UE dotyczące ochrony danych.

Po ustanowieniu ram Komisja zachęci zainteresowane strony do skupienia się na trzech obszarach priorytetowych:

- Bezpieczeństwo zastosowań o znaczeniu krytycznym lub wysokiego ryzyka[21]: systemy, od których jesteśmy zależni w codziennej działalności, począwszy od samochodów po urządzenia w zakładach produkcyjnych; od największych systemów takich jak samoloty lub elektrownie do najmniejszych, takich jak sprzęt medyczny, stają się w coraz większym stopniu cyfrowe i wzajemnie połączone. Dlatego kluczowe elementy ICT w takich produktach i systemach wymagają rygorystycznej oceny bezpieczeństwa.

- Bezpieczeństwo cybernetyczne w zakrojonych na szeroką skalę produktach, sieciach, systemach i usługach cyfrowych, takich jak szyfrowanie poczty elektronicznej, zapory sieciowe i wirtualne sieci prywatne, wykorzystywanych na równi przez sektor prywatny i publiczny do obrony przed atakami cybernetycznymi i wywiązywanie się z obowiązków regulacyjnych[22]; niezwykle istotne jest, aby rozpowszechnienie takich narzędzi nie prowadziło do nowych źródeł ryzyka lub nowych luk w zabezpieczeniach.

- Uwzględnianie bezpieczeństwa już w fazie projektowania w przypadku niedrogich, cyfrowych połączonych wzajemnie urządzeń dla masowego konsumenta, które wchodzą w skład internetu rzeczy: systemy objęte tym ramami mogłyby sygnalizować, że produkty są zbudowane przy wykorzystaniu najnowszych bezpiecznych metod projektowania, że zostały poddane odpowiednim próbom bezpieczeństwa i że sprzedawcy zobowiązali się do aktualizacji oprogramowania w przypadku nowo wykrytych luk w zabezpieczeniach oraz zagrożeń.

W priorytetach tych należy w szczególności uwzględniać zmieniający się krajobraz zagrożeń bezpieczeństwa cybernetycznego, a także znaczenie podstawowych usług, takich jak transport, energetyka, opieka zdrowotna, bankowość, infrastruktura rynków finansowych, infrastruktura dostaw wody pitnej bądź infrastruktura cyfrowa[23].

Mimo że nie można zagwarantować, że dany produkt, system bądź usługa ICT są w 100 % bezpieczne, istnieje kilka dobrze udokumentowanych i powszechnie znanych wad w projektowaniu produktów ICT, które mogą być wykorzystywane do ataków. Podejście zgodne z zasadą bezpieczeństwa już w fazie projektowania, przyjęte przez producentów urządzeń podłączonych do internetu, oprogramowania i sprzętu zagwarantuje uwzględnienie

---

[20] COM(2016) 176.

[21] Wyjątkiem byłaby sytuacja, w której obowiązkowa lub dobrowolna certyfikacja jest uregulowana w innych unijnych aktach prawnych.

[22] Na przykład dyrektywa (UE) 2016/1148, rozporządzenia (UE) 2016/679, dyrektywa (UE) 2015/2366 oraz inne proponowane akty prawne, takie jak Europejski kodeks łączności elektronicznej, wymagają od organizacji wprowadzenia stosownych środków bezpieczeństwa w celu uwzględnienia odnośnych postaci ryzyka cybernetycznego.

[23] Sektory objęte dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

bezpieczeństwa cybernetycznego przed skierowaniem nowego produktu do sprzedaży. Mogłoby to stanowić część „obowiązku dochowania należytej staranności", którego zasady byłyby następnie rozwijane we współpracy z branżą. Dzięki temu ograniczono by luki w zabezpieczeniach produktów/oprogramowania poprzez zastosowanie szeregu metod od projektowania po testowanie i weryfikację, łącznie z weryfikacją formalną w stosownych przypadkach, długookresową konserwacją oraz zastosowaniem bezpiecznych procesów cyklu życia, a także opracowywaniem aktualizacji i poprawek, aby rozwiązać wcześniej ukryte problemy i szybko aktualizować oraz dokonywać napraw[24]. Zwiększyłoby to również zaufanie konsumentów do produktów cyfrowych.

Poza tym należy uznać znaczącą rolę naukowców z sektora bezpieczeństwa cybernetycznego, działających na potrzeby osób trzecich, w wykrywaniu luk w zabezpieczeniach istniejących produktów i usług; należy też stworzyć warunki ułatwiające skoordynowane ujawnianie luk w zabezpieczeniach[25] we wszystkich państwach członkowskich w oparciu o najlepsze praktyki[26] i odpowiednie normy[27].

Jednocześnie **poszczególne sektory** borykają się ze specyficznymi kwestiami i należy je zachęcać do rozwoju własnych sposobów działania. W ten sposób ogólne strategie bezpieczeństwa cybernetycznego zostałyby uzupełnione o sektorowe strategie bezpieczeństwa w takich dziedzinach jak usługi finansowe[28], energetyka, transport i opieka zdrowotna[29].

Komisja wskazała już konkretne kwestie dotyczące **odpowiedzialności** wynikające z nowych technologii cyfrowych[30], a prace nad analizą konsekwencji są już w toku; kolejne etapy zostaną zakończone do czerwca 2018 r. Bezpieczeństwo cybernetyczne pociąga za sobą kwestie przypisania odpowiedzialności za szkody poniesione przez przedsiębiorstwa i łańcuch dostaw, a brak rozwiązania tych problemów utrudni rozwój silnego jednolitego rynku produktów i usług związanych z bezpieczeństwem cybernetycznym.

Rozwój unijnego jednolitego rynku zależy także od uwzględnienia bezpieczeństwa cybernetycznego w polityce w dziedzinie handlu i inwestycji. Skutki zagranicznego zakupu technologii o znaczeniu krytycznym – czego ważnym przykładem jest bezpieczeństwo cybernetyczne – są kluczowym aspektem ram w odniesieniu do **kontroli bezpośrednich inwestycji zagranicznych w Unii Europejskiej**[31], których celem jest umożliwienie monitorowania inwestycji z krajów trzecich pod kątem bezpieczeństwa i porządku publicznego. Jednocześnie wymagania w zakresie bezpieczeństwa cybernetycznego już

---

[24] Bezpieczeństwo cybernetyczne na europejskim jednolitym rynku cyfrowym, grupa wysokiego szczebla doradców naukowych, marzec 2017

[25] Skoordynowane wykrywanie luk w zabezpieczeniach jest formą współpracy, która umożliwia naukowcom zajmującym się bezpieczeństwem cybernetycznym zgłaszanie zagrożeń posiadaczowi lub sprzedawcy systemu informatycznego i ułatwia im wykonywanie tego zadania, organizacjom zaś daje możliwość rozpoznawania zagrożenia i zaradzenia mu w sposób właściwy i na czas, zanim szczegółowe informacje o podatności na zagrożenie zostaną ujawnione stronom trzecim lub podane do wiadomości publicznej.

[26] Na przykład *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations* (Przewodnik po dobrych praktykach w zakresie wykrywania luk w zabezpieczeniach. Od wyzwań do zaleceń). ENISA, 2016.

[27] ISO/IEC 29147:2014 Information technology – Security techniques –-Vulnerability disclosure (Technologia informatyczna – Techniki zabezpieczeń – Ujawnienie luk w zabezpieczeniach).

[28] Przyszłe prace Komisji dotyczące technologii finansowej obejmą bezpieczeństwo cybernetycznego dla sektora finansowego.

[29] W sektorze energetycznym na przykład łączenie bardzo starych i najnowszych technologii, zwłaszcza z powstającymi w czasie rzeczywistym wymaganiami sieci elektroenergetycznej.

[30] COM(2017) 228.

[31] COM(2017) 478.

stworzyły bariery handlowe dla unijnych towarów i usług w ważnych sektorach w wielu gospodarkach państw trzecich. Unijne ramy certyfikacji bezpieczeństwa cybernetycznego dodatkowo wzmocnią pozycję Europy na arenie międzynarodowej; ich dopełnieniem powinny być stałe działania na rzecz opracowania światowych norm wysokiego poziomu bezpieczeństwa oraz porozumień o wzajemnym uznawaniu.

2.3 Pełne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji

Główne narzędzia służące zwalczaniu zagrożeń cybernetycznych spoczywają obecnie w rękach podmiotów krajowych; UE uznała natomiast potrzebę podniesienia standardów. Incydenty cybernetyczne na dużą skalę rzadko dotykają tylko jedno państwo członkowskie ze względu na coraz bardziej zglobalizowany, uzależniony od aspektów cyfrowych i wzajemnych powiązań charakter takich kluczowych sektorów jak bankowość, energetyka bądź transport.

Dyrektywa o ochronie sieci i informacji jest pierwszym ogólnounijnym aktem prawnym w dziedzinie bezpieczeństwa cybernetycznego[32]. Opracowano ją w celu zbudowania odporności poprzez poprawę krajowych zdolności w zakresie bezpieczeństwa cybernetycznego; usprawnienia wzajemnej współpracy państw członkowskich; oraz stworzenia wobec przedsiębiorstw w ważnych sektorach gospodarki wymogu przyjęcia skutecznych praktyk w zakresie zarządzania ryzykiem oraz zgłaszania poważnych incydentów właściwym organom krajowym. Obowiązki te mają również zastosowanie wobec trzech rodzajów dostawców kluczowych usług internetowych: podmiotów oferujących operacje w chmurze, wyszukiwarek internetowych i internetowych platform handlowych. Celem tego wymogu jest ukształtowanie silniejszego i bardziej systematycznego podejścia oraz poprawa przepływu informacji.

Pełne wdrożenie dyrektywy przez wszystkie państwa członkowskie UE do maja 2018 r. ma zasadnicze znaczenie dla odporności UE na zagrożenia cybernetyczne. Proces ten jest wspierany przez zbiorowe działania państw członkowskich, które doprowadzą najpóźniej na jesień 2017 r. do sformułowania wytycznych wspomagających lepszą harmonizację wdrażania, zwłaszcza w odniesieniu do operatorów usług kluczowych. W ramach niniejszego pakietu poświęconego bezpieczeństwu cybernetycznemu Komisja publikuje również komunikat[33], mający wesprzeć jej działania za pomocą przedstawienia najlepszych praktyk z państw członkowskich, mających znaczenie dla wdrożenia dyrektywy, oraz wytycznych dotyczących jej funkcjonowania w praktyce.

Obszarem, w odniesieniu do którego dyrektywa wymaga uzupełnienia, jest przepływ informacji. Dyrektywa obejmuje mianowicie jedynie kluczowe sektory strategiczne – logiczne jest jednak, że potrzebne byłoby podobne podejście ze strony wszystkich zainteresowanych stron narażonych na ataki cybernetyczne; umożliwiłoby ono systematyczną ocenę podatności na zagrożenia i punktów przedostawania się sprawców takich ataków do systemów. Poza tym współpraca i wymiana informacji pomiędzy sektorem publicznym i prywatnym napotyka szereg przeszkód. Rządy i organy publiczne zajmujące się kwestiami bezpieczeństwa cybernetycznego niechętnie dzielą się odnośnymi informacjami w obawie przed narażeniem na szwank bezpieczeństwa narodowego lub konkurencyjności. Przedsiębiorstwa prywatne są oporne w dzieleniu się informacjami na temat swojej podatności na zagrożenia cybernetyczne i wynikających z nich strat z obawy przed ujawnieniem poufnych informacji biznesowych, ryzykiem utraty reputacji bądź złamaniem

[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[33] COM(2017) 476.

zasad ochrony danych[34]. Należy wzmocnić zaufanie wobec partnerstw publiczno-prywatnych, aby zbudować podstawy szerszej współpracy i wymiany informacji pomiędzy większą liczbą sektorów. Szczególnie ważną rolę w budowaniu zaufania niezbędnego do wymiany informacji między sektorem prywatnym i publicznym odgrywają ośrodki wymiany i analizy informacji. Poczyniono już pierwsze kroki w odniesieniu do poszczególnych sektorów o znaczeniu krytycznym, takich jak lotnictwo, przez powołanie Europejskiego Centrum ds. Bezpieczeństwa Cybernetycznego w Lotnictwie[35], oraz w energetyce przez rozwój ośrodków wymiany i analizy informacji[36]. Komisja przyczyni się w pełni do tego podejścia przy wsparciu ENISA; przyspieszenie jest niezbędne w szczególności w odniesieniu do sektorów świadczących usługi kluczowe, jak określono w dyrektywie w sprawie bezpieczeństwa sieci i informacji.

2.4 Odporność dzięki szybkiemu reagowaniu w sytuacji kryzysowej

Gdy dojdzie do ataku cybernetycznego, szybkie i skuteczne reagowanie może ograniczać jego skutki. Może również pokazać, że organy publiczne nie są bezbronne wobec ataków cybernetycznych i przyczynić się do budowania zaufania. Jeżeli chodzi o reagowanie samych instytucji unijnych ataki cybernetyczne należy przede wszystkim włączyć do istniejących mechanizmów zarządzania kryzysowego UE: zintegrowanego unijnego reagowania na poziomie politycznym w sytuacjach kryzysowych, koordynowanego przez prezydencję Rady[37] oraz ogólnych unijnych systemów szybkiego ostrzegania[38]. Potrzeba zareagowania na szczególnie poważny incydent lub atak cybernetyczny może być wystarczającą podstawą do sięgnięcia przez państwo członkowskie po unijną klauzulę solidarności[39].

Szybkie i skuteczne reagowanie zależy również od sprawnych mechanizmów wymiany informacji między wszystkimi kluczowymi podmiotami na szczeblu krajowym i unijnym, co z kolei wymaga jasności w kwestii ich ról i obowiązków. Komisja przeprowadziła konsultacje z instytucjami i państwami członkowskimi na temat planu działania, mającego na celu zapewnienie efektywnego przebiegu reakcji operacyjnej na szczeblu Unii i państw członkowskich na incydenty cybernetyczne na dużą skalę. W **planie działania** przedstawionym w zaleceniu[40] w ramach niniejszego pakietu objaśniono, w jaki sposób bezpieczeństwo cybernetyczne jest włączane do istniejących mechanizmów zarządzania kryzysowego na szczeblu unijnym, oraz określono cele i sposoby współpracy między państwami członkowskimi oraz między państwami członkowskimi a odpowiednimi

---

[34] Bezpieczeństwo cybernetyczne na europejskim jednolitym rynku cyfrowym, grupa wysokiego szczebla doradców naukowych, marzec 2017 Kwestią szczególną jest tajemnica handlowa. W komunikacie pt. „Wzmacnianie europejskiego systemu odporności cybernetycznej" z lipca 2016 r. odnotowano opór w stosunku do zgłaszania cyberkradzieży tajemnic przedsiębiorstwa oraz podkreślono znaczenie zaufanych kanałów sprawozdawczości zapewniających poufność.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa

[36] Działają nienastawione na osiąganie zysku organizacje oparte na aktywności swoich członków, tworzone przez podmioty prywatne i publiczne w celu wymiany informacji na temat zagrożeń cybernetycznych, ryzyka, zapobiegania, ograniczania skutków i reagowania. Zob. też ośrodki wymiany i analizy informacji w sektorze energetycznym (http://www.ee-isac.eu)

[37] Umożliwia to koordynację na najwyższym politycznym poziomie reagowania na poważne kryzysy międzysektorowe.

[38] To z kolei pozwala na wewnętrzną wymianę informacji oraz koordynację w kwestii pojawiających się kryzysów wielosektorowych lub też w obliczu przewidywanej bądź nieuchronnej groźby ich wystąpienia, które wymagają działań na szczeblu UE.

[39] Na podstawie art. 222 Traktatu o funkcjonowaniu Unii Europejskiej.

[40] C(2017) 6100.

instytucjami, służbami. agencjami i organami UE[41] podczas reagowania na incydenty cybernetyczne na dużą skalę i kryzysy cybernetyczne. W zaleceniu wezwano też państwa członkowskie i instytucje UE do ustanowienia ram reagowania kryzysowego UE w zakresie kryzysów cybernetycznych w celu zapewnienia wykonalności planu działania. Plan będzie regularnie poddawany sprawdzianom w ramach ćwiczeń z zakresu bezpieczeństwa cybernetycznego i innych form zarządzania kryzysowego[42] oraz aktualizowany w razie potrzeby.

Z uwagi na fakt, że incydenty cybernetyczne mogą w znacznym stopniu wpływać na funkcjonowanie gospodarki i codzienne życie obywateli, jednym z wariantów byłoby zbadanie możliwości stworzenia **funduszu pomocy w cybernetycznych sytuacjach kryzysowych** na wzór innych takich mechanizmów kryzysowych w innych dziedzinach unijnej polityki. Pozwoliłoby to państwom członkowskim zwrócić się o pomoc na szczeblu UE w trakcie lub w następstwie poważnego incydentu, pod warunkiem że dane państwo członkowskie wprowadziło wcześniej ostrożnościowy system bezpieczeństwa cybernetycznego, obejmujący pełne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz dojrzałe zarządzanie ryzykiem i ramy nadzoru na szczeblu krajowym. Taki fundusz, uzupełniając istniejące mechanizmy zarządzania kryzysowego na szczeblu unijnym, mógłby uruchomić zdolności szybkiego reagowania w interesie działań solidarnościowych i pokryć koszty specyficznych działań w sytuacji kryzysowej, takich jak usunięcie wyposażenia, którego integralność została naruszona, lub zastosowanie narzędzi ograniczających skutki bądź narzędzi reagowania w oparciu o krajowe doświadczenie zgodnie z Unijnym Mechanizmem Ochrony Ludności.

2.5 Sieć kompetencji w dziedzinie bezpieczeństwa cybernetycznego oraz Europejskie Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego

Narzędzia technologiczne do celów bezpieczeństwa cybernetycznego są wartościami strategicznymi, a także kluczowymi technologiami przyszłego wzrostu gospodarczego. W strategicznym interesie UE leży zapewnienie, aby Unia utrzymała i rozwijała podstawowe zdolności do ochrony gospodarki cyfrowej, cyfrowego społeczeństwa i demokracji cyfrowej, zabezpieczania sprzętu i oprogramowania o znaczeniu krytycznym oraz dostarczania kluczowych usług w zakresie bezpieczeństwa cybernetycznego.

Partnerstwo publiczno-prywatne w dziedzinie bezpieczeństwa cybernetycznego[43] utworzone w 2016 r. było pierwszym ważnym krokiem, dającym impuls do inwestycji o wartości 1,8 mld EUR do 2020 r. Skala inwestycji realizowanych obecnie w innych częściach świata[44] sugeruje jednak, że UE musi zwiększyć wysiłki w zakresie inwestycji i przezwyciężyć rozproszenie potencjału na obszarze całej Unii.

W obliczu poziomu zaawansowania technologii bezpieczeństwa cybernetycznego, skali niezbędnych inwestycji oraz potrzeby rozwiązań funkcjonujących na obszarze całej Unii UE może zaoferować wartość dodaną. W oparciu o działania państw członkowskich i partnerstwa

---

[41] W tym Europol, ENISA, unijny zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) oraz Centrum Analiz Wywiadowczych UE (INTCEN).

[42] Na przykład przeprowadzanych przez ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[43] C(2016) 4400 final.

[44] Tylko w 2017 r. Stany Zjednoczone zamierzają zainwestować w bezpieczeństwo cybernetyczne 19 mld USD, co stanowi wzrost o 35 % w porównaniu z rokiem 2016. Biuro Rzecznika Prasowego Prezydenta USA: 'Fact Sheet: Cybersecurity National Action Plan' (Zestawienie informacji: Narodowy plan bezpieczeństwa cybernetycznego), 9 lutego 2016 r.

publiczno-prywatnego kolejnym krokiem będzie wzmocnienie unijnych zdolności w dziedzinie bezpieczeństwa cybernetycznego przez tworzenie **sieci ośrodków kompetencji w dziedzinie bezpieczeństwa cybernetycznego**[45] z **Europejskim Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego** na czele. Sieć ta wraz z Centrum będą pobudzać rozwój technologii w dziedzinie bezpieczeństwa cybernetycznego i jej rozpowszechnianie oraz uzupełniać budowanie zdolności w tym obszarze na szczeblu unijnym i krajowym. Komisja zainicjuje ocenę skutków w celu przeanalizowania możliwych wariantów, w tym możliwości powołania wspólnego przedsięwzięcia, z zamiarem określenia jego struktury w 2018 r.

Pierwszym krokiem i podstawą przyszłych rozważań będzie propozycja Komisji zainicjowania fazy pilotażowej w ramach programu „Horyzont 2020", aby pomóc w tworzeniu sieci ośrodków krajowych; nadałoby to nowy impet rozwijaniu kompetencji w dziedzinie bezpieczeństwa cybernetycznego i postępowi w dziedzinie technologii. W tym celu Komisja zamierza przedłożyć propozycję krótkookresowego zasilenia finansowego w wysokości 50 mln EUR. Działanie to uzupełni trwającą realizację partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa cybernetycznego.

Skomasowanie i profilowanie prac badawczych byłoby centralnym elementem sieci i początkowym przedmiotem głównego zainteresowania Centrum. Aby wspomóc rozwijanie zdolności przemysłowych, Centrum mogłoby też działać jako kierownik projektu, zdolny do obsługi projektów międzynarodowych. Byłoby to dodatkowym bodźcem dla innowacyjności i konkurencyjności unijnego przemysłu UE na arenie światowej w rozwoju nowoczesnych technologii cyfrowych nowej generacji, w tym sztucznej inteligencji, kwantowych technologii obliczeniowych, łańcucha bloków i bezpiecznej tożsamości cyfrowej, a także w zagwarantowaniu dostępu do danych masowych dla wszystkich przedsiębiorstw z siedzibą w UE. Wszystkie te technologie mają kluczowe znaczenie dla bezpieczeństwa cybernetycznego w przyszłości. Centrum korzystałoby także z działań UE na rzecz rozszerzania infrastruktury na potrzeby wysokowydajnych technologii obliczeniowych: ma to kluczowe znaczenie dla analizy dużych ilości danych, szybkiego szyfrowania i odszyfrowywania danych, sprawdzania tożsamości, symulacji ataków cybernetycznych oraz analizy materiałów wideo[46].

Sieć ośrodków kompetencji może również dysponować zdolnościami do wspierania przemysłu poprzez próby i symulacje stanowiące podstawę do certyfikacji bezpieczeństwa cybernetycznego opisanej w sekcji 2.2. Jej włączenie w pełny zakres unijnej działalności w zakresie bezpieczeństwa cybernetycznego zagwarantowałoby nieprzerwaną aktualizację kierunków jej prac w zależności od potrzeb. Celem Centrum byłoby propagowanie stosowania wysokich standardów bezpieczeństwa cybernetycznego nie tylko w dziedzinie technologii i systemów bezpieczeństwa cybernetycznego, ale także w ramach rozwijania umiejętności cyfrowych na wysokim poziomie na potrzeby zawodowe, przez zapewnianie rozwiązań i modeli krajowych działań na rzecz upowszechniania umiejętności cyfrowych. W tym zakresie wzmocniłoby to także zdolności w dziedzinie bezpieczeństwa cybernetycznego na szczeblu UE oraz pozwoliło wykorzystać efekt synergii zwłaszcza z ENISA, CERT-UE, Europolem, ewentualnym przyszłym funduszem pomocy w cybernetycznych sytuacjach kryzysowych i krajowymi CSIRT.

[45] Sieć obejmowałaby istniejące i przyszłe ośrodki bezpieczeństwa cybernetycznego utworzone w państwach członkowskich, w których skład wchodziłyby zwykle publiczne podmioty badawcze i laboratoria.

[46] COM(2012) 45 final i COM(2016) 178 final.

Szczególnie istotnym przedmiotem działań sieci ośrodków kompetencji musi być rozwiązanie kwestii braku europejskich zdolności w zakresie oceny **szyfrowania** produktów i usług, z których korzystają obywatele, przedsiębiorstwa i rządy w ramach jednolitego rynku cyfrowego. Silne szyfrowanie jest podstawą bezpiecznych systemów identyfikacji cyfrowej, które odgrywają kluczową rolę w skutecznym zapewnianiu bezpieczeństwa cyfrowego[47]. Zapewnia ono również bezpieczeństwo własności intelektualnej i umożliwia ochronę praw podstawowych, takich jak wolność wypowiedzi i prawo do ochrony danych osobowych; stanowi również gwarancję bezpiecznego handlu internetowego[48]

Ponieważ unijne rynki cywilnego i wojskowego bezpieczeństwa cybernetycznego stoją w obliczu wspólnych wyzwań[49], a technologie podwójnego zastosowania wymagają ścisłej współpracy w obszarach o szczególnym znaczeniu, drugi etap tworzenia sieci i jej Centrum można by rozszerzyć o wymiar dotyczący obrony cybernetycznej, z pełnym poszanowaniem postanowień Traktatu dotyczących wspólnej polityki bezpieczeństwa i obrony. Oprócz skupienia się na kwestiach technologicznych, wymiar obronny mógłby przyczynić się do poprawy współpracy między państwami członkowskimi w dziedzinie obrony cybernetycznej, obejmującej wymianę informacji, orientację sytuacyjną, rozwijanie wiedzy specjalistycznej i skoordynowanego reagowania oraz wspomóc państwa członkowskie w budowaniu wspólnych zdolności. Mógłby odgrywać również rolę platformy, umożliwiając państwom członkowskim określanie priorytetów unijnej obrony cybernetycznej, służąc analizie wspólnych rozwiązań, przyczyniając się do opracowywania wspólnych strategii, pomagając w organizowaniu wspólnych szkoleń, ćwiczeń i prób na szczeblu unijnym oraz wspierając działania z zakresu taksonomii i norm bezpieczeństwa cybernetycznego; Centrum przypadłaby rola wspierająca i doradcza. Aby wykonywać opisane powyżej działania Centrum musiałoby współpracować ściśle i w pełnej komplementarności z Europejską Agencją Obrony w dziedzinie obrony cybernetycznej, a także z ENISA w zakresie odporności na zagrożenia cybernetyczne. W tym wymiarze obronnym należałoby także uwzględnić proces zainicjowany przez dokument otwierający debatę na temat przyszłości europejskiej obronności.

Wysoki poziom odporności niezbędny w zakresie obronności cybernetycznej wymaga szczególnego ukierunkowanie wysiłków badawczych i technologicznych. Projekty w zakresie obrony cybernetycznej lub technologie opracowane przez przedsiębiorstwa mogłyby korzystać z Europejskiego Funduszu Obronnego, z którego środków w stosownych przypadkach pochodziłoby finansowanie zarówno na etapie badań, jak również rozwoju[50]. Konkretne obszary, takie jak systemy szyfrowania oparte na technologiach kwantowych, orientacja sytuacyjna w odniesieniu do cyberprzestrzeni, systemy kontroli dostępu w oparciu o dane biometryczne, wykrywanie zaawansowanych uporczywych zagrożeń bądź eksploracja danych mogą być szczególnie istotne w tym kontekście. Wysoki Przedstawiciel, Europejska Agencja Obrony i Komisja będą wspierać państwa członkowskie w określaniu obszarów, w których wspólne projekty dotyczące bezpieczeństwa cybernetycznego mogłyby być wzięte pod uwagę pod kątem finansowania z Europejskiego Funduszu Obronnego.

---

[47] Już w ramach programu „Horyzont 2020” Komisja rozpisze nowy konkurs Horizon Prize, w którym nagroda w wysokości 4 mln EUR przypadnie autorowi (autorom) najlepszego innowacyjnego rozwiązania w zakresie metod płynnego uwierzytelniania w internecie.

[48] Bezpieczeństwo cybernetyczne na europejskim jednolitym rynku cyfrowym, grupa wysokiego szczebla doradców naukowych, marzec 2017

[49] *Study on synergies between the civilian and the defence cybersecurity markets* (Badanie na temat synergii między cywilnym a wojskowym rynkiem bezpieczeństwa cybernetycznego” (Optimity; SMART 2014-0059).

[50] Już obecnie program rozwoju europejskiego przemysłu obronnego nada priorytet projektom z dziedziny obrony przed atakami cybernetycznymi, a obrona cybernetyczna będzie jednym z tematów zaproszenia do składania wniosków ogłoszonego w 2018 r.

2.6 Budowanie silnej unijnej bazy umiejętności cybernetycznych

Edukacja stanowi ważny aspekt bezpieczeństwa cybernetycznego. Skuteczne zapewnianie bezpieczeństwa cybernetycznego w znacznym stopniu zależy od umiejętności ludzi. Przewiduje się jednak, że niedobór wykwalifikowanej kadry w zakresie bezpieczeństwa cybernetycznego w sektorze prywatnym w Europie wyniesie w 2022 r. 350 000 osób[51]. Edukację w zakresie bezpieczeństwa cybernetycznego należy rozwijać na wszystkich poziomach, zaczynając od regularnych szkoleń pracowników w zakresie obrony cybernetycznej przez dodatkowe szkolenia dla wszystkich specjalistów ICT po nowe specyficzne programy nauczania z dziedziny bezpieczeństwa cybernetycznego. Należy powołać silne akademickie ośrodki kompetencji, aby zaspokoić potrzeby w zakresie kształcenia i szkolenia w trybie przyspieszonym; ośrodki te mogłyby korzystać ze wskazówek Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego oraz ENISA. Celem powinno być doprowadzenie do sytuacji, w której uwzględnianie zasad bezpieczeństwa cybernetycznego w projektowaniu produktów i systemów ICT będzie oczywiste od samego początku. Edukacja w zakresie bezpieczeństwa cybernetycznego nie powinna się ograniczać tylko do specjalistów ICT, ale należy ją włączyć do programów nauczania w innych obszarach, takich jak inżynieria, zarządzanie lub prawo, a także do sektorowych ścieżek kształcenia. Nauczycieli i uczniów już w szkołach podstawowych i średnich należy uwrażliwiać na kwestie cyberprzestępczości i bezpieczeństwa cybernetycznego w ramach uzyskiwania umiejętności cyfrowych w szkołach.

Unia Europejska wraz z państwami członkowskimi powinna także wnieść wkład w te wysiłki w oparciu o działalność Koalicji na rzecz umiejętności cyfrowych i zatrudnienia[52] oraz za pomocą ustanowienia na przykład systemów staży dla MŚP w zakresie bezpieczeństwa cybernetycznego.

2.7 Propagowanie higieny cybernetycznej i świadomości zagrożeń

W przypadku około 95 % incydentów można powiedzieć, że doszło do nich z powodu „pewnego rodzaju błędu ludzkiego – zamierzonego lub niezamierzonego”[53]; czynnik ludzki odgrywa istotną rolę. Zatem odpowiedzialność za bezpieczeństwo cybernetyczne spoczywa na każdym z nas. Oznacza to, że zachowanie pracowników, przedsiębiorstw i administracji publicznej musi ulec zmianie, aby zagwarantować powszechne zrozumienie zagrożeń i wyposażenie wszystkich w narzędzia i umiejętności niezbędne do szybkiego wykrywania ataków i aktywnej ochrony przed nimi. Ludzie muszą rozwinąć nawyki higieny cybernetycznej, a przedsiębiorstwa i organizacje muszą przyjąć właściwe programy bezpieczeństwa cybernetycznego oparte na analizie ryzyka i regularnie je aktualizować, aby odzwierciedlały one zmieniający się krajobraz zagrożeń.

W dyrektywie w sprawie bezpieczeństwa sieci i informacji nie tylko określono obowiązki państw członkowskich w zakresie wymiany informacji na temat ataków cybernetycznych na szczeblu unijnym, ale także nałożono na nie wymóg opracowania przemyślanych krajowych strategii bezpieczeństwa cybernetycznego oraz ram w zakresie bezpieczeństwa sieci

[51] Ogólnoświatowe badanie na temat pracowników w sektorze bezpieczeństwa informacyjnego, 2017. Ogólny niedobór na świecie wynosi 1,8 mln osób.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM „The Cybersecurity Intelligence Index” 2014, o którym mowa w Securitymagazine.com, 19 czerwca 2014 r.

i systemów. Administracja publiczna na szczeblu UE i na szczeblu krajowym powinna odgrywać przewodnią rolę w pobudzaniu dalszych postępów.

Po pierwsze: państwa członkowskie powinny maksymalnie zwiększyć dostępność narzędzi w dziedzinie bezpieczeństwa cybernetycznego dla przedsiębiorstw i osób fizycznych. W szczególności należy zwiększyć wysiłki na rzecz zapobiegania cyberprzestępczości i ograniczania jej skutków dla użytkowników końcowych. Przykładem jest już działanie Europolu w ramach kampanii „NoMoreRansom" (Nigdy więcej okupu)[54], stworzonej w wyniku ścisłej współpracy między organami ścigania a przedsiębiorstwami z obszaru bezpieczeństwa cybernetycznego, aby pomóc użytkownikom w zapobieganiu zarażeniom wirusami oprogramowania szantażującego i odszyfrowywaniu danych, w przypadku gdy staną się ofiarami ataku. Systemy takie powinny zostać rozszerzone na inne typy złośliwego oprogramowania, a UE powinna opracować **pojedynczy portal w celu zgromadzenia wszystkich takich narzędzi w punkcie kompleksowej obsługi**, oferując użytkownikom doradztwo z zakresu zapobiegania atakom i wykrywania złośliwego oprogramowania oraz linki do mechanizmów ich zgłaszania.

Po drugie: państwa członkowskie powinny przyspieszyć **stosowanie bezpieczniejszych pod względem cybernetycznym narzędzi w rozwoju administracji elektronicznej** i również w pełni korzystać z sieci kompetencji. Należy propagować przyjmowanie bezpiecznych środków identyfikacji w oparciu o unijne ramy prawne w zakresie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, które obowiązują od 2016 r. i zapewniają przewidywalne otoczenie regulacyjne w celu umożliwienia bezpiecznych i sprawnych interakcji przedsiębiorstw, obywateli i władz publicznych[55]. Ponadto instytucje publiczne, zwłaszcza podmioty świadczące usługi kluczowe, powinny zapewnić swoim pracownikom przeszkolenie z dziedzin związanych z bezpieczeństwem cybernetycznym.

Po trzecie: państwa członkowskie powinny nadać priorytet kwestii świadomości zagrożeń cybernetycznych za pomocą **kampanii informacyjnych**, w tym adresowanych do szkół, uczelni wyższych, społeczności przedsiębiorców i instytucji badawczych. Obchodzony każdego roku w październiku miesiąc bezpieczeństwa cybernetycznego, którego przebieg jest koordynowany przez ENISA, zostanie rozszerzony, tak aby zwiększyć jego zasięg jako wspólnego działania informacyjnego na szczeblu unijnym i krajowym. Równie ważne jest podnoszenie poziomu świadomości w odniesieniu do internetowych **kampanii dezinformacyjnych i fałszywych informacji** w mediach społecznościowych, ukierunkowanych w szczególności na podważanie procesów demokratycznych i europejskich wartości. Odpowiedzialność spoczywa w pierwszym rzędzie na podmiotach na szczeblu krajowym – także w odniesieniu do wyborów do Parlamentu Europejskiego – łączenie wiedzy specjalistycznej i wymiana doświadczeń na szczeblu unijnym okazało się jednak wartością dodaną w zakresie koncentracji na działaniu[56].

---

54 https://www.nomoreransom.org/.

55 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, przyjęte w dniu 23 lipca 2014 r. Komisja Europejska zapewnia także elementy składowe i narzędzia na potrzeby interoperacyjności identyfikacji elektronicznej i podpisu elektronicznego (np. zaufane wyszukiwarki internetowe; ang. *Trusted Lists Browsers*) za pośrednictwem programu inicjatywy „Łącząc Europę"

56 Przykładem jest utworzenie zespołu zadaniowego East StratCom Task Force, powołanego w 2015 r. przez państwa członkowskie i Wysokiego Przedstawiciela w celu przeciwdziałania kampaniom dezinformacyjnym prowadzonym przez Rosję. Zespół jest zaangażowany w opracowywanie produktów w dziedzinie komunikacji i kampanie nakierowane na wyjaśnianie polityki UE w regionie Partnerstwa Wschodniego.

Także **przemysł** jako całość ma do odegrania ważną rolę, ze szczególnym naciskiem jednak na producentów i dostawców usług cyfrowych. Wymaga to zapewnienia użytkownikom (obywatelom, przedsiębiorstwom i administracji publicznej) narzędzi, dzięki którym będą mogli wziąć odpowiedzialność za własne działania w internecie, i uświadomienia im, że zachowywanie higieny cybernetycznej jest niezbędnym elementem oferty dla konsumentów[57]. Aby wykrywać i eliminować słabe punkty, przemysł powinien dążyć do posiadania wewnętrznych procedur postępowania w zakresie badania, selekcji i rozwiązywania kwestii podatności na zagrożenia, niezależnie od tego, czy potencjalne zagrożenie pochodzi ze źródła zewnętrznego, czy wewnętrznego.

Kluczowe działania

- Pełne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji.
- Sprawne przyjęcie przez Parlament Europejski i Radę rozporządzenia ustanawiającego nowy mandat ENISA oraz europejskie ramy certyfikacji[58].
- Wspólna inicjatywa Komisji i przemysłu na rzecz określenia zasady „obowiązku dochowania należytej staranności" w celu zmniejszenia luk w zabezpieczeniach produktów/oprogramowania oraz propagowania zasady „bezpieczeństwa na etapie projektowania".
- Sprawne wdrożenie planu reagowania na wypadek wystąpienia poważnego incydentu transgranicznego.
- Zainicjowanie oceny skutków w celu przeanalizowania możliwości złożenia w 2018 r. przez Komisję wniosku w sprawie ustanowienia sieci ośrodków kompetencji w zakresie bezpieczeństwa cybernetycznego oraz Europejskiego Centrum Badań i Kompetencji w zakresie Bezpieczeństwa Cybernetycznego, w oparciu o uruchomioną niezwłocznie fazę pilotażową.
- Wsparcie państw członkowskich w określaniu obszarów, w ramach których wspólne projekty z dziedziny bezpieczeństwa cybernetycznego mogą być wzięte pod uwagę pod kątem finansowania z Europejskiego Funduszu Obronnego.
- Ogólnoeuropejski punkt kompleksowej obsługi do udzielania pomocy ofiarom ataków cybernetycznych, dostarczający informacji na temat najnowszych zagrożeń i skupiający porady praktyczne oraz narzędzia bezpieczeństwa cybernetycznego.
- Działania podejmowane przez państwa członkowskie w celu włączenia bezpieczeństwa cybernetycznego do programów rozwoju umiejętności, administracji cyfrowej i kampanii informacyjnych.
- Działania podejmowane przez przemysł w celu przyspieszenia szkoleń dla swoich pracowników w zakresie bezpieczeństwa cybernetycznego oraz przyjęcie podejścia zgodnego z zasadą „bezpieczeństwo na etapie projektowania" w odniesieniu do oferowanych przez przemysł produktów, usług i procesów.

3. KSZTAŁTOWANIE SKUTECZNEJ UNIJNEJ PREWENCJI CYBERNETYCZNEJ

Skuteczna prewencja oznacza ustanowienie systemu środków, które będą jednocześnie wiarygodne i zniechęcające potencjalnych cyberprzestępców i sprawców ataków cybernetycznych. Dopóki sprawcy ataków cybernetycznych – zarówno podmioty państwowe

[57] Niektórzy wytwórcy są już oswojeni z tą koncepcją, gdyż w pewnych przepisach unijnych dotyczących produktów (takie jak dyrektywa 2006/42/WE w sprawie maszyn) wprowadzono zasady „bezpieczeństwa na etapie projektowania".

[58] COM(2017) 477.

jak i niepaństwowe – mogą się obawiać co najwyżej niepowodzenia, dopóty niewiele może zniechęcać ich do podejmowania kolejnych prób. Skuteczniejsze reagowanie organów ścigania, skoncentrowane na wykrywaniu, śledzeniu i ściganiu cyberprzestępców, ma zasadnicze znaczenie dla kształtowania skutecznej unijnej prewencji. Dochodzi do tego potrzeba wpierania przez UE państw członkowskich w rozwoju zdolności podwójnego zastosowania w zakresie bezpieczeństwa cybernetycznego. Falę ataków cybernetycznych zaczniemy odwracać dopiero wtedy, gdy zwiększymy prawdopodobieństwo schwytania i ukarania sprawców. W przypadku ataków cybernetycznych dochodzenia należy przeprowadzać niezwłocznie, a ich sprawców doprowadzać przed oblicze wymiaru sprawiedliwości, lub podejmować działania umożliwiające odpowiednią reakcję polityczną lub dyplomatyczną. W sytuacji wystąpienia poważnego kryzysu o istotnym wymiarze międzynarodowym i obronnym, Wysoki Przedstawiciel może przedłożyć Radzie warianty odpowiedniego reagowania.

Kroki w kierunku poprawy prawa karnego w odpowiedzi na ataki cybernetyczne zostały już poczynione wraz z przyjęciem w 2013 r. dyrektywy dotyczącej ataków na systemy informatyczne[59]. Ustanowiono w niej minimalne zasady dotyczące definicji przestępstw i sankcji w dziedzinie ataków na systemy informatyczne oraz określono środki operacyjne w celu poprawy współpracy między organami. Dyrektywa przyczyniła się do osiągnięcia istotnych postępów w procesie zapewniania zbliżonego poziomu kategoryzacji ataków cybernetycznych jako przestępstw we wszystkich państwach członkowskich, co sprzyja współpracy transgranicznej między organami ścigania prowadzącymi dochodzenia w sprawie tego rodzaju przestępstw. Potencjał dyrektywy nie został jeszcze jednak w pełni wykorzystany – zakres jej oddziaływania mógłby zostać zwiększony, gdyby państwa członkowskie w pełni wdrożyły wszystkie jej przepisy[60]. Komisja będzie nadal zapewniać wsparcie państwom członkowskim we wdrażaniu dyrektywy i obecnie nie widzi potrzeby składania wniosku o dokonanie w niej zmian.

3.1 Identyfikacja podmiotów działających w złych intencjach

Aby zwiększyć nasze szanse na pociągnięcie sprawców do odpowiedzialności, musimy pilnie poprawić naszą zdolność do identyfikacji osób odpowiedzialnych za ataki cybernetyczne. Znalezienie użytecznych informacji na potrzeby dochodzeń związanych z cyberprzestępczością, przeważnie w postaci śladów cyfrowych, jest największym wyzwanie dla organów ścigania. Musimy zatem zwiększyć nasze zdolności technologiczne do skutecznego prowadzenia dochodzeń przez wzmocnienie jednostki Europolu ds. cyberprzestępczości o specjalistów z tej dziedziny. Europol stał się głównym podmiotem wspierającym państwa członkowskie w dochodzeniach w sprawach wykraczających poza jeden obszar jurysdykcji. Powinien zatem stać się centrum wiedzy fachowej dla organów ścigania w zakresie dochodzeń i informatyki śledczej *online*.

Rozpowszechniona praktyka ukrywania wielu użytkowników – czasami tysięcy z nich – za jednym adresem IP bardzo utrudnia z technicznego punktu widzenia dochodzenie w sprawach szkodliwych zachowań w sieci. Czasem powoduje też konieczność, np. w przypadku poważnych przestępstw takich jak wykorzystywanie seksualne dzieci, zbadania bardzo wielu użytkowników w celu identyfikacji jednego podmiotu działającego w złych intencjach. Dlatego UE będzie zachęcać do stosowania nowego protokołu (IPv6), gdyż pozwala on na przydzielenie jednego użytkownika na adres IP, z wyraźnym pożytkiem dla organów ścigania

[59] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne.

[60] COM(2017) 474.

i dochodzeń w zakresie bezpieczeństwa cybernetycznego. Pierwszym krokiem zachęcającym do jego wprowadzenia będzie nadanie przez Komisję priorytetu kwestii przechodzenia na IPv6 w obrębie swoich polityk, w tym wymogów dotyczących zamówień publicznych, finansowania projektów i badań, oraz wspieranie koniecznych materiałów szkoleniowych. Ponadto państwa członkowskie powinny rozważyć zawarcie dobrowolnych porozumień z dostawcami usług internetowych w celu stymulowania stosowania IPv6.

Belgia zajmuje czołową pozycję na świecie[61] *pod względem wskaźnika przyjęcia IPv6 również dzięki współpracy publiczno-prywatnej: odnośne zainteresowane strony uznały ograniczenie stosowania jednego adresu IP do maksymalnie 16 użytkowników w ramach dobrowolnych środków samoregulacyjnych, które stanowiły zachętę do przejścia na IPv6*[62].

Mówiąc bardziej ogólnie, należy w większym stopniu propagować odpowiedzialność w internecie. Oznacza to propagowanie środków przeciwdziałających nadużyciom nazw domen do dystrybucji niezamówionych komunikatów lub ataków phishingowych. W tym celu Komisja będzie działać na rzecz poprawy funkcjonowania systemów nazw domen i adresów IP WHOIS[63] oraz dostępności i dokładności zawartych w nich informacji, wspierając przy tym wysiłki Internetowej Korporacji ds. Nadawania Nazw i Numerów[64].

3.2 Doskonalenie reagowania przez organy ścigania

Skuteczne prowadzenie **dochodzeń** i **ściganie** przestępczości wykorzystującej cyberprzestrzeń jest kluczowym czynnikiem prewencji wobec ataków cybernetycznych. Obecne ramy proceduralne wymagają jednak lepszego dostosowania do potrzeb ery internetu[65]. Szybkość ataków cybernetycznych może okazać się zbyt duża dla obecnych procedur, a także stworzyć specyficzne potrzeby w zakresie sprawnej współpracy transgranicznej. W tym celu – jak ogłoszono w Europejskiej agendzie bezpieczeństwa – Komisja na początku 2018 r. przedstawi wnioski w celu ułatwienia **transgranicznego dostępu do elektronicznego materiału dowodowego**. Równolegle Komisja wprowadza w życie praktyczne środki, służące do poprawy transgranicznego dostępu do elektronicznego materiału dowodowego ma potrzeby dochodzeń w sprawach karnych, obejmujące finansowanie szkoleń w zakresie współpracy transgranicznej, rozwijanie elektronicznej platformy wymiany informacji w UE oraz standaryzację form współpracy sądowej między państwami członkowskimi.

Inną przeszkodą dla skutecznego ścigania są różne procedury kryminalistyczne gromadzenia elektronicznego materiału dowodowego w ramach dochodzeń dotyczących przestępstw cybernetycznych w różnych państwach członkowskich. Takiemu stanowi rzeczy można

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf

63 Protokół oparty na zasadzie pytanie/odpowiedź, który jest szeroko stosowany do wysyłania zapytań do baz danych przechowujących dane na temat zarejestrowanych użytkowników lub właścicieli zasobów internetowych.

64 Internetowa Korporacja ds. Nadawania Nazw i Numerów (ICANN) jest nienastawioną na zysk organizacją, odpowiedzialną za koordynację obsługi technicznej i procedur kilku baz danych związanych z przestrzeniami nazw w internecie.

65 Jednym z przykładów może być (wirtualny) serwer typu C&C (ang. *command and control*) zarządzający botnetem Avalanche, który przemieszczał fizyczne serwery i domeny co pięć minut.

zaradzić przez działania na rzecz ustanowienia wspólnych standardów kryminalistycznych. Ponadto aby wspomóc tropienie i typowanie sprawców, należy wzmocnić potencjał kryminalistyczny. Jednym z kroków w tym kierunku byłoby dalsze rozwijanie potencjału kryminalistycznego w Europolu polegające na dostosowaniu istniejących zasobów budżetowych i ludzkich w działającym przy tej agencji Europejskim Centrum ds. Walki z Cyberprzestępczością w celu sprostania rosnącemu zapotrzebowaniu na wsparcie operacyjne w transgranicznych dochodzeniach dotyczących cyberprzestępczości. Inne działanie polegałoby na przyjęciu przedstawionego powyżej ukierunkowania na potencjał technologiczny w dziedzinie szyfrowania przez przyjrzenie się, jak jego nadużywanie przez przestępców staje się poważnym wyzwaniem w walce z poważną przestępczością, w tym z terroryzmem i cyberprzestępczością. Komisja przedstawi wyniki dotychczasowych refleksji na temat **roli szyfrowania w dochodzeniach w sprawach karnych**[66] do października 2017 r.[67]

Z uwagi na nieuznający granic charakter internetu ramy międzynarodowej współpracy określone w **budapeszteńskiej Konwencji Rady Europy o cyberprzestępczości**[68] umożliwiają zróżnicowanej grupie państw stosowanie najlepszych standardów prawnych w odniesieniu do różnych krajowych przepisów dotyczących cyberprzestępczości. Obecnie badane są możliwości dodania do Konwencji protokołu[69], który stanowiłby korzystną okazję do zajęcia się kwestią transgranicznego dostępu do elektronicznego materiału dowodowego w kontekście międzynarodowym. Zamiast tworzyć nowe międzynarodowe instrumenty prawne UE wzywa jednak raczej wszystkie państwa do opracowywania stosownych przepisów krajowych i dążenia do współpracy w ramach istniejących ram międzynarodowych.

Powszechna dostępność narzędzi służących do zapewnienia anonimowości ułatwia przestępcom ukrywanie się. **Ukryta sieć**, tzw. darknet[70], otwiera przed przestępcami nowe możliwości dostępu do materiałów przedstawiających seksualne wykorzystywanie dzieci, do narkotyków bądź broni palnej, często stwarzające niewielkie ryzyko schwytania[71]. Jest ona obecnie kluczowym źródłem narzędzi stosowanych w cyberprzestępczości, takich jak złośliwe oprogramowanie i narzędzia hakerskie. Komisja wspólnie z odnośnymi zainteresowanymi stronami przeanalizuje krajowe koncepcje w celu wskazania nowych rozwiązań. Europol powinien ułatwiać i wspierać dochodzenia w sprawie ukrytej sieci, oceniać zagrożenia i pomagać w określeniu jurysdykcji i priorytetowym traktowaniu spraw

---

66 Prezydencja Rady: Wyniki posiedzenia Rady ds. Sprawiedliwości i Spraw Wewnętrznych w dniach 8 i 9 grudnia 2016 r., nr 15391/16.

67 Ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa a dnia 29 czerwca 2017 r. (COM(2017) 354 final).

68 Konwencja jest pierwszym międzynarodowym traktatem w sprawie przestępstw popełnianych za pośrednictwem internetu oraz innych sieci komputerowych i zajmuje się głównie naruszeniami praw autorskich, oszustwami internetowymi, pornografią dziecięcą i naruszeniem bezpieczeństwa sieci. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 W 2017 r. 55 rządów ratyfikowało Konwencję Rady Europy o cyberprzestępczości bądź do niej przystąpiło.

69 Warunki przygotowania projektu 2. protokołu dodatkowego do konwencji budapeszteńskiej o cyberprzestępczości, T-CY (2017)3.

70 Ukryta sieć składa się z treści w nakładających się sieciach, które korzystają z internetu, ale wymagają szczególnego oprogramowania, skonfigurowania lub autoryzacji, aby można było do nich uzyskać dostęp. Ukryta sieć stanowi niewielką część sieci głębokiej: tej części sieci, która nie jest przeszukiwana przez wyszukiwarki.

71 Godnym uwagi wyjątkiem jest niedawne zamknięcie dwóch największych przestępczych rynków darknetu: AlphaBay i Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

wysokiego ryzyka, a UE może odegrać kluczową rolę w koordynacji działań międzynarodowych[72].

Rosnącym obszarem przestępczej działalności cybernetycznej jest bezprawne wykorzystywanie danych kart kredytowych lub innych elektronicznych systemów płatności. Dane uwierzytelniające płatności uzyskane w wyniku ataków internetowych przeciwko sprzedawcom detalicznym lub innym legalnym przedsiębiorstwom są następnie sprzedawane w internecie i mogą być wykorzystywane przez przestępców w celu popełniania nadużyć[73]. Komisja przedstawia wniosek w celu wzmocnienia prewencji przez wdrożenie **dyrektywy w sprawie zwalczania oszustw i fałszerstw bezgotówkowych środków płatniczych**[74]. Posłuży on do aktualizacji istniejących przepisów w tej dziedzinie i wzmocnieniu zdolności egzekwowania prawa w celu przeciwdziałania tego rodzaju przestępczości.

Zdolności dochodzeniowe organów ścigania państw członkowskich również wymagają udoskonalenia, należy także podnieść poziom wiedzy prokuratorów i sędziów na temat przestępczości wykorzystującej cyberprzestrzeń oraz możliwości dochodzeniowych. Eurojust i Europol przyczyniają się do osiągnięcia tego celu oraz do poprawy koordynacji działań, w ścisłej współpracy z wyspecjalizowanymi grupami doradczymi w obrębie działającego przy Europolu Centrum ds. Walki z Cyberprzestępczością i sieci szefów jednostek ds. walki z cyberprzestępczością oraz prokuratorów specjalizujących się w ściganiu cyberprzestępczości. Komisja przeznaczy 10,5 mln EUR na finansowanie zwalczania cyberprzestępczości, przede wszystkim w ramach **instrumentu na rzecz współpracy policyjnej swojego Funduszu Bezpieczeństwa Wewnętrznego**. Szkolenie jest ważnym elementem i w ramach europejskiej Grupy Szkolenia i Edukacji w zakresie Cyberprzestępczości opracowano szereg użytecznych materiałów. Należy je teraz szeroko rozpowszechnić wśród specjalistów z organów ścigania, przy wsparciu Agencji Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania Przestępczości (CEPOL).

3.3 Publiczno-prywatna współpraca w zwalczaniu cyberprzestępczości

Skuteczność tradycyjnych mechanizmów ścigania przestępstw została podważona przez cechy świata cyfrowego, który składa się głównie z infrastruktury będącej własnością prywatną i wielu różnych podmiotów działających w obrębie wielu różnych jurysdykcji. W rezultacie współpraca z sektorem prywatnym, w tym przemysłem i społeczeństwem obywatelskim, ma fundamentalne znaczenie dla skutecznego zwalczania przestępczości przez organy publiczne. W związku z tym sektor finansowy także ma kluczowe znaczenie i należy zacieśnić współpracę. Należy na przykład wzmocnić rolę jednostek wywiadu finansowego[75] w odniesieniu do cyberprzestępczości.

Niektóre państwa członkowskie podjęły już pewne działania. W Niderlandach instytucje finansowe i organy ścigania pracują wspólnie nad rozwiązaniem problemu oszustw internetowych i cyberprzestępczości w ramach grupy zadaniowej ds. przestępczości

[72] Europol odgrywa już istotną rolę w tej dziedzinie. Najnowszy przykład: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[73] Oszustwa są ważnym źródłem dochodów dla przestępczości zorganizowanej i w związku z tym czynnikiem ułatwiającym innego rodzaju działalność przestępczą, taką jak terroryzm, handel narkotykami i handel ludźmi.

[74] COM(2017) 489.

[75] Jednostki wywiadu finansowego pełnią rolę krajowych ośrodków przyjmowania i analizowania zgłoszeń o podejrzanych transakcjach oraz innych informacji istotnych w kontekście prania pieniędzy, powiązanych przestępstw źródłowych oraz finansowania terroryzmu, a także mają za zadanie rozpowszechnianie wyników tej analizy.

elektronicznej. Niemiecki ośrodek kompetencji do walki z cyberprzestępczością stanowi operacyjny punkt węzłowy dla swoich członków do celów wymiany informacji w ścisłej współpracy z biurem niemieckiej policji federalnej i opracowuje środki, których celem jest zapewnienie ochrony przed cyberprzestępczością. W 16 państwach członkowskich[76] utworzono centra doskonałości w zakresie cyberprzestępczości, aby ułatwić współpracę między organami ścigania, sektorem akademickim i partnerami prywatnymi przy opracowywaniu i wymianie najlepszych praktyk, szkoleniach i budowaniu potencjału.
Komisja wspiera powoływanie partnerstw publiczno-prywatnych oraz mechanizmów współpracy za pośrednictwem specjalnych projektów, takich jak internetowe centrum ds. oszustw cybernetycznych[77], które wdraża model wymiany informacji i norm w celu przeanalizowania i ograniczenia zagrożeń ze strony przestępczości elektronicznej oraz oszustw internetowych.

W związku z cyberprzestępczością przedsiębiorstwa prywatne muszą być w stanie wymieniać z organami ścigania informacje na temat konkretnych incydentów – w tym dane osobowe – przy pełnym poszanowaniu przepisów dotyczących ochrony danych. W ramach reformy unijnych przepisów o ochronie danych, która wejdzie w życie w maju 2018 r., określono wspólny zbiór przepisów ustanawiających warunki, na jakich mogą ze sobą współpracować organy ścigania oraz podmioty prywatne. Komisja Europejska będzie współpracować z Europejską Radą Ochrony Danych i z odpowiednimi zainteresowanymi stronami, aby określić najlepsze praktyki w tej dziedzinie i w stosownych przypadkach wydawać wytyczne.

3.4 Doskonalenie reagowania politycznego

W niedawno przyjętych **ramach wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne**[78] („zestaw narzędzi dla dyplomacji cyfrowej”) określono środki w ramach wspólnej polityki zagranicznej i bezpieczeństwa, w tym środki ograniczające, które można zastosować do wzmocnienia możliwości reagowania przez UE na działania zagrażające jej politycznym i ekonomicznym interesom oraz bezpieczeństwu. Ramy te stanowią ważny krok w rozwoju zdolności do sygnalizowania i reagowania na szczeblu UE i państw członkowskich. Zwiększą one naszą zdolność do przypisania sprawstwa szkodliwych działań cybernetycznych, co umożliwi wywarcie wpływu na zachowanie potencjalnych agresorów, z uwzględnieniem potrzeby zapewnienia proporcjonalnych reakcji. Przypisanie państwu lub podmiotowi niepaństwowemu sprawstwa pozostaje suwerenną decyzją polityczną podjętą na podstawie danych wywiadowczych pozyskanych ze wszystkich możliwych źródeł. Obecnie trwają prace z państwami członkowskimi nad wdrażaniem ram, które będą kontynuowane w ścisłej koordynacji z planem reagowania na incydenty cybernetyczne na dużą skalę[79]. Informacje na potrzeby orientacji sytuacyjnej, niezbędnej do zastosowania środków ujętych w ramach, powinny być gromadzone, analizowane

[76] Austria, Belgia, Bułgaria, Cypr, Estonia, Francja, Grecja, Hiszpania, Irlandia, Litwa, Niemcy, Polska, Republika Czeska, Rumunia, Słowenia i Zjednoczone Królestwo.
[77] Inicjatywa EU-OF2CEN ma na celu umożliwienie systematycznej, ogólnounijnej wymiany informacji pomiędzy bankami a organami ścigania, aby zapobiec płatnościom na rzecz oszustów i „słupów”, oraz na potrzeby prowadzenia dochodzeń i ścigania sprawców dopuszczających się tych czynów. Jest ona współfinansowana przez UE (instrument na rzecz współpracy policyjnej Funduszu Bezpieczeństwa Wewnętrznego).
[78] http://www.consilium.europa.eu/pl/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/
[79] C(2017) 6100.

i wymieniane w INTCEN[80], w ścisłej współpracy z państwami członkowskimi i instytucjami unijnymi.

3.5 Kształtowanie prewencji w zakresie bezpieczeństwa cybernetycznego za pomocą potencjału obronnego państw członkowskich

Państwa członkowskie rozwijają już zdolności w zakresie obrony cybernetycznej. Ponadto, z uwagi na zatarcie granic między obroną cybernetyczną a bezpieczeństwem cybernetycznym oraz charakter podwójnego zastosowania narzędzi i technologii cybernetycznych, a także znaczne różnice między podejściami państw członkowskich, UE jest właściwym podmiotem, mogącym wspomagać efekt synergii działań wojskowych i cywilnych[81].

Państwa członkowskie dysponujące bardziej zaawansowanymi zdolnościami w zakresie bezpieczeństwa cybernetycznego i zainteresowane ich zespoleniem mogłyby rozważyć, przy wsparciu Wysokiego Przedstawiciela, Komisji i Europejskiej Agencji Obrony, włączenie obrony cybernetycznej w ramy „stałej współpracy strukturalnej" (PESCO). Mogłoby to być oparte na działaniach określonych powyżej, mających na celu pobudzenie unijnego potencjału przemysłowego i strategicznej autonomii. UE może również wspierać interoperacyjność, w tym przez ułatwianie rozwoju zdolności, koordynacji szkoleń i edukacji oraz działania normalizacyjne w zakresie podwójnego zastosowania.

Należy również w pełni wykorzystać wspólne ramy reagowania na zagrożenia hybrydowe, które często obejmują ataki cybernetyczne, w szczególności za pośrednictwem komórki UE ds. syntezy informacji o zagrożeniach hybrydowych oraz niedawno utworzonego Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach, którego misja polega na zachęcaniu do strategicznego dialogu i prowadzeniu badań oraz analiz.

UE nada nowy impuls uchwalonym w 2014 r. ramom polityki UE w zakresie cyberobrony[82], stanowiącym narzędzie do dalszej integracji w sektorze bezpieczeństwa cybernetycznego i obrony w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO). Kluczowe znaczenie ma odporność na zagrożenia cybernetyczne w obrębie samych misji i operacji WPBiO: opracowane zostaną znormalizowane procedury i zdolności techniczne, które mogłyby wesprzeć zarówno będące w toku misje i operacje cywilne i wojskowe, jak też odnoszące się do nich struktury planowania i realizacji oraz dostawców technologii i usług informatycznych na potrzeby ESDZ. Aby zapewnić postęp współpracy państw członkowskich i lepsze ukierunkowanie wysiłków UE w tej dziedzinie, Europejska Agencja Obrony i ESDZ, we współpracy ze służbami Komisji, będą ułatwiać zaangażowanie na poziomie strategicznym osób odpowiedzialnych w państwach członkowskich za podejmowanie decyzji w dziedzinie obrony cybernetycznej. UE będzie również wspierać rozwój europejskich rozwiązań z zakresu bezpieczeństwa cybernetycznego w ramach swoich działań na rzecz bazy technologiczno-przemysłowej na potrzeby europejskiej obronności. Obejmuje to również wspieranie regionalnych klastrów doskonałości w dziedzinie bezpieczeństwa cybernetycznego i obronności.

Służby Komisji, działając w ścisłej współpracy z ESDZ, państwami członkowskimi i innymi właściwymi organami UE, udostępnią do 2018 r. **platformę szkoleń i edukacji w dziedzinie obrony cybernetycznej**, aby zlikwidować istniejący w tym obszarze niedobór wykwalifikowanych kadr. Będzie to uzupełnieniem prac Europejskiej Agencji Obrony w tej

[80] JOIN(2016) 018 final.

[81] UE postrzega cyberprzestrzeń jako obszar operacji, podobnie jak w przypadku operacji lądowych, powietrznych i morskich. Działania z dziedziny obrony cybernetycznej obejmują także ochronę i odporność systemów kosmicznych oraz powiązanej infrastruktury naziemnej.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515

dziedzinie i pomoże rozwiązać problem istniejącego obecnie niedoboru kwalifikacji w zakresie bezpieczeństwa cybernetycznego i obrony cybernetycznej.

Kluczowe działania

- Inicjatywa Komisji na rzecz transgranicznego dostępu do elektronicznego materiału dowodowego (na początku 2018 r.).
- Sprawne przyjęcie przez Parlament Europejski i Radę proponowanej dyrektywy w sprawie zwalczania oszustw i fałszowania bezgotówkowych środków płatniczych.
- Wprowadzenie wymogów w zakresie IPv6 w unijnych zamówieniach publicznych, badaniach i finansowaniu projektów. Dobrowolne porozumienia między państwami członkowskimi a dostawcami usług internetowych w celu poprawy wdrażania IPv6.
- Zrewidowane/rozszerzone podejście w Europolu do informatyki śledczej i monitorowania ukrytej sieci.
- Wdrożenie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne.
- Wzmocnione wsparcie finansowe na rzecz krajowych i międzynarodowych projektów poprawy wymiaru sprawiedliwości w sprawach karnych w cyberprzestrzeni.
- Uruchomienie w 2018 r. platformy edukacyjnej poświęconej bezpieczeństwu cybernetycznemu w celu wyeliminowania istniejącego obecnie niedoboru kwalifikacji w zakresie bezpieczeństwa cybernetycznego i obrony cybernetycznej.

4. WZMOCNIENIE WSPÓŁPRACY MIĘDZYNARODOWEJ W DZIEDZINIE BEZPIECZEŃSTWA CYBERNETYCZNEGO

Kształtowana w oparciu o zasadnicze wartości UE i prawa podstawowe, takie jak prawo do swobodnego wyrażania poglądów i prawo do prywatności i ochrony danych osobowych, oraz o zasadę propagowania otwartej, wolnej i bezpiecznej cyberprzestrzeni unijna polityka w dziedzinie bezpieczeństwa cybernetycznego ma na celu podjęcie wciąż zmieniających się wyzwań związanych ze wspieraniem globalnej stabilności cybernetycznej, a także przyczynia się do strategicznej autonomii Europy w cyberprzestrzeni.

4.1 Bezpieczeństwo cybernetyczne w stosunkach zewnętrznych

Dostępne dowody wskazują na to, że ludzie na całym świecie uważają ataki cybernetyczne z innych państw za jedno z głównych zagrożeń dla bezpieczeństwa narodowego[83]. Z uwagi na globalny charakter tego zagrożenia zawieranie i utrzymywanie trwałych sojuszy i partnerstw z państwami trzecimi ma zasadnicze znaczenie dla zapobiegania i powstrzymywania ataków cybernetycznych – stających się coraz bardziej centralnymi kwestiami w zapewnianiu stabilności i bezpieczeństwa w wymiarze międzynarodowym. UE nada priorytet ustanowieniu strategicznych ram na rzecz zapobiegania konfliktom i zapewniania stabilizacji w cyberprzestrzeni w ramach swych relacji dwustronnych, regionalnych i wielostronnych oraz opartych na porozumieniu wielu zainteresowanych stron.

UE silnie propaguje stanowisko, w myśl którego prawo międzynarodowe, a w szczególności Karta Narodów Zjednoczonych, ma zastosowanie w odniesieniu do cyberprzestrzeni. Jako uzupełnienie wiążących przepisów prawa międzynarodowego UE przyjmuje dobrowolne niewiążące normy, reguły i zasady odpowiedzialnego zachowania ze strony państwa, które zostały określone przez grupę ekspertów rządowych ONZ[84]. Zachęca ona także do rozwijania

[83] Wiosna 2017 r., Światowe badanie poglądów, Pew Research Centre.
[84] A/68/98 i A/70/174.

i wdrażania regionalnych środków budowy zaufania, zarówno w obrębie Organizacji Bezpieczeństwa i Współpracy w Europie, jak również i w innych rejonach.

Na poziomie relacji dwustronnych kontynuowane będą dialogi poświęcone kwestiom cyberprzestrzeni[85], uzupełnione działaniami na rzecz ułatwienia współpracy z państwami trzecimi w celu wzmocnienia zasad należytej staranności i odpowiedzialności państwa w cyberprzestrzeni. UE potraktuje priorytetowo zagadnienia bezpieczeństwa międzynarodowego w cyberprzestrzeni w ramach swoich międzynarodowych zobowiązań, zarazem jednak zapewniając, aby bezpieczeństwo cybernetyczne nie stało się pretekstem do ochrony rynku oraz ograniczania podstawowych praw i wolności, w tym wolności słowa i dostępu do informacji. Kompleksowe podejście do bezpieczeństwa cybernetycznego wymaga poszanowania praw człowieka i Unia będzie nadal stać na straży podstawowych wartości w wymiarze globalnym w oparciu o wytyczne UE w sprawie praw człowieka dotyczące wolności wypowiedzi w internecie[86]. W tym względzie UE podkreśla znaczenie zaangażowania wszystkich zainteresowanych stron w zarządzanie internetem.

Komisja przedstawiła również wniosek[87] dotyczący unowocześnienia unijnej kontroli wywozu, uwzględniający wprowadzenie kontroli wywozu technologii inwigilacji o znaczeniu krytycznym, które mogłyby powodować naruszenia praw człowieka lub być używane do celów zagrażających bezpieczeństwu samej UE, i zintensyfikuje dialog z państwami trzecimi w celu propagowania spójności i odpowiedzialnego zachowania w tej dziedzinie w wymiarze światowym.

4.2 Budowanie zdolności w obszarze bezpieczeństwa cybernetycznego

Bezpieczeństwo cybernetyczne w wymiarze globalnym zależy od lokalnych i krajowych zdolności wszystkich państw do zapobiegania incydentom cybernetycznym i reagowania na nie oraz wykrywania i ścigania przypadków cyberprzestępczości. Działania wspierające krajowe wysiłki na rzecz budowania odporności w państwach trzecich zwiększą poziom bezpieczeństwa cybernetycznego w wymiarze globalnym, co przyniesie pozytywne skutki dla UE. Przeciwdziałanie szybko zmieniającym się zagrożeniom cybernetycznym wymaga szkoleń, opracowania działań politycznych i prac prawodawczych, a także sprawnie funkcjonujących zespołów reagowania na incydenty bezpieczeństwa komputerowego oraz jednostek ścigania cyberprzestępczości we wszystkich krajach świata.

Od 2013 r. UE przewodzi międzynarodowej budowie zdolności w obszarze bezpieczeństwa cybernetycznego i systematycznie wiąże te działania z prowadzoną przez siebie współpracą na rzecz rozwoju. UE będzie w dalszym ciągu wspierać model budowania zdolności oparty na przestrzeganiu praw, zgodnie z podejściem określonym w strategii „Digital4Development”[88]. Priorytetem w zakresie budowania zdolności będą kraje unijnego sąsiedztwa i kraje rozwijające się, które doświadczają szybkiego rozwoju sieci połączeń i szybkiego wzrostu zagrożeń. Działania UE będą stanowić uzupełnienie unijnego programu działań na rzecz rozwoju w świetle programu działań na rzecz zrównoważonego rozwoju do roku 2030 oraz ogólnych działań na rzecz budowania zdolności instytucjonalnych.

Aby poprawić zdolności UE do wykorzystania jej wspólnej wiedzy specjalistycznej do wspierania budowania zdolności, należy powołać unijną sieć w zakresie budowania zdolności

[85] We wrześniu 2017 r. UE prowadziła dialogi poświęcone kwestiom cyberprzestrzeni z USA, Chinami, Japonią, Republiką Korei i Indiami.
[86] Wytyczne UE w sprawie praw człowieka dotyczące wolności wypowiedzi w internecie i poza nim
[87] COM(2016) 616.
[88] SWD(2017) 157.

cybernetycznych, skupiającą ESDZ, organy państw członkowskich odpowiedzialne za bezpieczeństwo cybernetyczne, agencje UE, służby Komisji, środowisko akademickie i społeczeństwo obywatelskie. Aby pomóc w zapewnieniu lepszych wskazówek politycznych i ustalenia hierarchii działań UE na rzecz wsparcia państw trzecich, opracowane zostaną unijne wytyczne w zakresie budowania zdolności cybernetycznych.

UE będzie również współpracować z innymi podmiotami aktywnymi w tym zakresie, aby uniknąć dublowania działań i umożliwić bardziej ukierunkowane budowanie zdolności w różnych regionach.

4.3 WSPÓŁPRACA UE-NATO

W oparciu o osiągnięte już znaczne postępy UE pogłębi swoją współpracę z NATO w dziedzinie bezpieczeństwa cybernetycznego, zagrożeń hybrydowych i obrony, zgodnie ze Wspólną deklaracją z dnia 8 lipca 2016 r.[89]. Priorytety obejmują wspomaganie interoperacyjności za pośrednictwem spójnych wymogów i norm w zakresie obrony cybernetycznej, wzmocnienie współpracy w zakresie szkoleń i ćwiczeń, harmonizację wymogów dotyczących kształcenia.

UE i NATO będą również umacniać współpracę na rzecz badań i innowacji w zakresie obrony cybernetycznej i rozwijać aktualne uzgodnienia techniczne dotyczące wymiany informacji w zakresie bezpieczeństwa cybernetycznego między swoimi organami odpowiedzialnymi za ten obszar[90]. Należy wykorzystać efekty najnowszych wspólnych wysiłków na rzecz przeciwdziałania zagrożeniom hybrydowym, zwłaszcza współpracy między komórką UE ds. syntezy informacji o zagrożeniach hybrydowych a działem NATO ds. analizy zagrożeń hybrydowych, aby wzmocnić odporność na kryzysy cybernetyczne i reagowanie w przypadku ich zaistnienia. Dalsza współpraca między UE a NATO będzie wspierana za pomocą ćwiczeń dotyczących obrony cybernetycznej, przy zaangażowaniu ESDZ i innych podmiotów unijnych oraz właściwych partnerów po stronie NATO, w tym Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi w Tallinnie. W 2017 r. NATO i UE po raz pierwszy przeprowadzą równoległe i skoordynowane ćwiczenia na podstawie scenariusza ataku hybrydowego, w których dowództwo obejmie NATO, a w 2018 r. podobne ćwiczenia odbędą się pod przewodnictwem UE. Kolejne sprawozdanie z postępów we współpracy między UE a NATO, które zostanie przedłożone odpowiednim Radom w grudniu 2017 r., stworzy okazję do rozważenia możliwości dalszego rozszerzania tej współpracy, zwłaszcza poprzez zapewnienie wspólnych, pewnych i stabilnych środków komunikacji między wszystkimi odnośnymi zaangażowanymi instytucjami i organami, w tym ENISA.

Kluczowe działania

- Rozwinięcie strategicznych ram zapobiegania konfliktom i umacnianie stabilizacji w cyberprzestrzeni.
- Utworzenie nowej sieci budowania zdolności w celu wsparcia zdolności państw trzecich do postępowania w przypadku zagrożeń cybernetycznych i opracowanie unijnych wytycznych w zakresie budowania zdolności cybernetycznych, służących lepszemu ustaleniu priorytetów działań UE.

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/

[90] CERT-UE i zespół reagowania na incydenty komputerowe NATO (NCIRC).

- Dalsza współpraca między UE a NATO, obejmująca uczestnictwo w równoległych i skoordynowanych ćwiczeniach oraz wzmocnienie interoperacyjności norm dotyczących bezpieczeństwa cybernetycznego.

5. PODSUMOWANIE

Gotowość UE do reagowania w obszarze bezpieczeństwa cybernetycznego ma zasadnicze znaczenie dla jednolitego rynku cyfrowego i naszej Unii Bezpieczeństwa i Obrony. Wzmocnienie europejskiego bezpieczeństwa cybernetycznego i przeciwdziałanie zagrożeniom dla celów zarówno cywilnych, jak i wojskowych, jest bezwzględną koniecznością.

Nadchodzący szczyt cyfrowy organizowany przez prezydencję estońską w dniu 29 września 2017 r. stanowi okazję do okazania wspólnej determinacji w nadaniu bezpieczeństwu cyfrowemu centralnej pozycji w UE jako społeczeństwie cyfrowym. W ramach tego wspólnego zaangażowania Komisja wzywa państwa członkowskie do podjęcia zobowiązań co do sposobów ich działania w obszarach, w których spoczywa na nich główna odpowiedzialność. Powinno to obejmować wzmocnienie bezpieczeństwa cybernetycznego przez:

- zapewnienie pełnego i skutecznego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji do dnia 9 maja 2018 r., a także zapewnienie zasobów niezbędnych organom publicznym odpowiedzialnym za bezpieczeństwo cybernetyczne do skutecznego wykonywania zadań;
- zastosowanie tych samych zasad do organów administracji publicznej ze względu na rolę, którą odgrywają w społeczeństwie i gospodarce jako całości;
- zapewnienie szkoleń w dziedzinie bezpieczeństwa cybernetycznego w administracji publicznej;
- nadanie priorytetu kwestii świadomości cybernetycznej w ramach kampanii informacyjnych i włączenie bezpieczeństwa cybernetycznego do programu kształcenia akademickiego i szkoleń zawodowych;
- wykorzystanie inicjatyw w sprawie stałej współpracy strukturalnej (PESCO) i Europejskiego Funduszu Obrony do wspierania rozwoju projektów w zakresie obrony cybernetycznej.

W niniejszym wspólnym komunikacie nakreślono skalę wyzwań i przedstawiono zakres środków, które UE może zastosować. Potrzebujemy Europy odpornej, która może skutecznie chronić swoich obywateli przez odpowiednio wczesne rozpoznanie ewentualnych incydentów cybernetycznych, budowanie silnych struktur ochrony i zachowania, szybkie przywracanie stanu sprzed ataku i odstraszanie agresorów. W niniejszym komunikacie zaproponowano ukierunkowane środki, które umożliwią dalsze wzmocnienie struktur i zdolności UE w zakresie bezpieczeństwa cybernetycznego w sposób skoordynowany, w pełnej współpracy z państwami członkowskimi i różnymi podmiotami unijnymi oraz przy poszanowaniu ich kompetencji i obowiązków. Wdrożenie jego postulatów będzie wyraźnym sygnałem, że UE i jej państwa członkowskie będą współpracować w celu ustanowienia poziomu bezpieczeństwa cybernetycznego adekwatnego do coraz większych wyzwań, przed którymi stoi dziś Europa.