KOMISJA
EUROPEJSKA

WYSOKI PRZEDSTAWICIEL UNII
EUROPEJSKIEJ DO SPRAW
ZAGRANICZNYCH I POLITYKI
BEZPIECZEŃSTWA

Bruksela, dnia 7.2.2013
JOIN(2013) 1 final

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

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej:

otwarta, bezpieczna i chroniona cyberprzestrzeń

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

Strategia bezpieczeństwa cybernetycznego Unii Europejskiej:

otwarta, bezpieczna i chroniona cyberprzestrzeń

1. WPROWADZENIE

1.1. Kontekst

W ciągu ostatnich dwóch dziesięcioleci internet oraz szerzej rozumiana cyberprzestrzeń miały olbrzymi wpływ na wszystkie aspekty funkcjonowania społeczeństwa. Nasze codzienne życie, prawa podstawowe, interakcje społeczne i gospodarka uzależnione są od sprawnie funkcjonujących technologii informacyjno-komunikacyjnych. Otwarta i wolna cyberprzestrzeń wspiera włączenie polityczne i społeczne na całym świecie, usuwa bariery między państwami, społecznościami i obywatelami, umożliwiając interakcję oraz wymianę informacji i pomysłów w skali światowej, stanowi forum, na którym promuje się wolność słowa i korzystanie z praw podstawowych, oraz daje społeczeństwom szansę na walkę o bardziej demokratyczne i sprawiedliwe rządy – co miało miejsce zwłaszcza podczas arabskiej wiosny.

Aby cyberprzestrzeń pozostała otwarta i wolna, w środowisku internetowym powinny mieć zastosowanie te same normy, zasady i wartości, które UE wspiera w świecie rzeczywistym. W cyberprzestrzeni należy zapewnić ochronę praw podstawowych, demokracji i praworządności. Nasza wolność i nasz dobrobyt w coraz większym stopniu uzależnione są od sprawnego i innowacyjnego internetu, który nadal będzie odgrywał kluczową rolę, jeżeli sektor prywatny i społeczeństwo obywatelskie będą w dalszym ciągu stymulować jego rozwój. Wolność w środowisku internetowym wymaga jednak również bezpieczeństwa i ochrony. Cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami, przy czym znaczącą rolę w zapewnieniu wolnej i bezpiecznej cyberprzestrzeni odgrywają administracje rządowe. Mają one szereg zadań: zapewnienie dostępu i otwartości, poszanowanie i ochronę praw podstawowych w internecie oraz utrzymanie niezawodności i interoperacyjności internetu. Znaczne części cyberprzestrzeni są jednak w posiadaniu i użytku sektora prywatnego i dlatego wszelkie inicjatywy w tej dziedzinie, jeśli mają prowadzić do sukcesów, muszą uwzględniać jego wiodącą rolę.

Technologie informacyjno-komunikacyjne stanowią obecnie fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu, na którym opierają się na wszystkie sektory gospodarki. Stanowią one obecnie podstawę złożonych systemów, które napędzają gospodarkę w takich kluczowych sektorach jak finanse, opieka zdrowotna, energetyka i transport; wiele modeli biznesowych opiera się na nieprzerwanej dostępności internetu i na sprawnym funkcjonowaniu systemów informatycznych.

Poprzez dokończenie tworzenia jednolitego rynku cyfrowego Europa mogłaby zwiększyć swój PKB o prawie 500 mld EUR rocznie[1], czyli średnio o 1000 EUR na osobę. Aby popularność zdobyły nowe technologie, takie jak płatności elektroniczne, chmury

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

obliczeniowe oraz komunikacja typu maszyna-maszyna[2], potrzebne będzie zaufanie i poczucie pewności ze strony obywateli. Niestety według badania Eurobarometru z 2012 r.[3] prawie jedna trzecia Europejczyków nie czuje się wystarczająco pewnie przy korzystaniu z internetu do celów operacji bankowych lub zakupów. Przeważająca większość stwierdziła również, że unika podawania danych osobowych w internecie ze względów bezpieczeństwa. W całej UE więcej niż co dziesiąty użytkownik internetu był już ofiarą oszustw internetowych.

W ostatnich latach można było zauważyć, że chociaż cyfrowy świat przynosi ogromne korzyści, jest również podatny na zagrożenia. Incydenty naruszające bezpieczeństwo cybernetyczne[4], zamierzone bądź przypadkowe, których liczba wzrasta w alarmującym tempie, mogą spowodować zakłócenia w świadczeniu podstawowych usług, które uznajemy za oczywiste, takich jak np. dostawy wody, usługi opieki zdrowotnej, dostawy energii elektrycznej i usługi telefonii komórkowej. Zagrożenia mogą mieć różne źródła – w tym przestępcze, motywowane politycznie, terrorystyczne lub inicjowane przez państwo, jak również mogą być efektem klęsk żywiołowych i niezamierzonych błędów.

Gospodarka UE pada już ofiarą cyberprzestępstw[5] popełnianych zarówno względem sektora prywatnego, jak i osób fizycznych. Cyberprzestępcy wykorzystują coraz bardziej zaawansowane metody ingerowania w struktury systemów informatycznych, wykradają krytyczne dane i żądają od przedsiębiorstw okupów. Nasilenie szpiegostwa gospodarczego i działań inicjowanych przez państwa w cyberprzestrzeni stanowi nową kategorię zagrożeń dla administracji rządowych i przedsiębiorstw w UE.

W krajach spoza UE rządy mogą również nadużywać cyberprzestrzeni w celu inwigilowania i kontrolowania własnych obywateli. UE może przeciwdziałać tej sytuacji poprzez promowanie swobód, a także zapewnianie przestrzegania praw podstawowych w internecie.

Wszystkie te czynniki pomagają zrozumieć, dlaczego rządy na całym świecie zaczęły opracowywać strategie bezpieczeństwa cybernetycznego i dlaczego uważają, że kwestie związane z cyberprzestrzenią stają się coraz bardziej istotnym problemem o wymiarze międzynarodowym. Nadszedł czas, aby UE zintensyfikowała działania w tej dziedzinie. W niniejszym wniosku dotyczącym strategii bezpieczeństwa cybernetycznego Unii Europejskiej, przedstawionym przez Komisję i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (Wysokiego Przedstawiciela), przedstawiono wizję UE w tej dziedzinie, wyjaśniono podział ról i obowiązków oraz określono działania, których celem jest

---

2 Na przykład rośliny z wbudowanymi czujnikami do przekazywania systemowi zraszającemu informacji o tym, że należy je podlać.

3 Specjalne badanie Eurobarometru nr 390 w sprawie cyberbezpieczeństwa (2012).

4 Bezpieczeństwo cybernetyczne ogólnie odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci i tę infrastrukturę uszkodzić. Bezpieczeństwo cybernetyczne polega na działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji.

5 Cyberprzestępczość ogólnie odnosi się do szerokiego wachlarza różnych rodzajów działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Cyberprzestępczość obejmuje tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług/systemów, oraz złośliwe oprogramowanie).

uczynienie środowiska internetowego w UE najbezpieczniejszym na świecie, w oparciu o skuteczną ochronę i wspieranie praw obywateli.

1.2. Zasady bezpieczeństwa cybernetycznego

Wolny od granic i wielowarstwowy internet stał się jednym z najpotężniejszych instrumentów umożliwiających globalny postęp bez nadzoru i regulacji ze strony administracji rządowych. Sektor prywatny powinien w dalszym ciągu odgrywać wiodącą rolę w tworzeniu internetu i w bieżącym zarządzaniu nim, ale równocześnie coraz bardziej oczywista staje się konieczność wprowadzenia wymogów w zakresie przejrzystości, odpowiedzialności i bezpieczeństwa. Niniejsza strategia ma na celu wyjaśnienie zasad, którymi należy się kierować przy opracowywaniu polityki w zakresie cyberbezpieczeństwa w UE i na arenie międzynarodowej.

Podstawowe wartości UE mają zastosowanie w świecie cyfrowym w taki sam sposób, jak w świecie fizycznym

Przepisy i normy mające zastosowanie w innych obszarach naszego codziennego życia mają również zastosowanie w odniesieniu do cyberprzestrzeni.

Ochrona praw podstawowych, wolności wypowiedzi, danych osobowych i prywatności

Zapewnienie cyberbezpieczeństwa będzie zadowalające i skuteczne tylko wtedy, kiedy będzie ono oparte na podstawowych prawach i swobodach zapisanych w Karcie praw podstawowych Unii Europejskiej oraz na podstawowych wartościach UE. Jednocześnie zabezpieczenie praw osób fizycznych nie jest możliwe bez bezpiecznych sieci i systemów. Wszelka wymiana informacji do celów bezpieczeństwa cybernetycznego w sytuacji, gdy w grę wchodzą dane osobowe, powinna być zgodna z unijnymi przepisami dotyczącymi ochrony danych i powinna w pełni uwzględniać prawa obywateli w tej dziedzinie.

Dostęp dla wszystkich

Ze względu na skalę wpływu świata cyfrowego na życie społeczne, ograniczony dostęp do internetu lub jego brak oraz nieumiejętność posługiwania się technologiami cyfrowymi stawiają obywateli w niekorzystnej sytuacji. Każdy powinien mieć możliwość dostępu do internetu i do niezakłóconego przepływu informacji. Aby umożliwić bezpieczny dostęp dla wszystkich, należy zagwarantować integralność i bezpieczeństwo internetu.

Demokratyczne i efektywne zarządzanie wielostronne

Cyfrowego świata nie kontroluje jeden podmiot. Obecnie istnieje szereg zainteresowanych stron, wśród których jest wiele podmiotów komercyjnych i pozarządowych, które zaangażowane są w bieżące zarządzanie zasobami, protokołami i normami internetowymi, a także przyszłym rozwojem internetu. UE ponownie podkreśla znaczenie, jakie ma udział wszystkich zainteresowanych stron w obecnym modelu zarządzania internetem, i popiera takie wielostronne podejście do zarządzania[6].

Wspólna odpowiedzialność za zapewnienie bezpieczeństwa

Coraz większa zależność od technologii informacyjno-komunikacyjnych we wszystkich dziedzinach życia doprowadziła do powstania słabych punktów, które należy właściwie

[6] Zob. również dokument COM(2009) 277 – Komunikat Komisji do Parlamentu Europejskiego i Rady pt. „Zarządzanie Internetem: kolejne działania".

określić, dokładnie przeanalizować oraz usunąć lub zneutralizować. Wszystkie właściwe podmioty – organy publiczne, sektor prywatny czy też pojedynczy obywatele – muszą uznać tę wspólną odpowiedzialność, podjąć działania zmierzające do zapewnienia sobie ochrony i w razie konieczności zapewnić skoordynowaną reakcję mającą na celu zwiększenie bezpieczeństwa cybernetycznego.

2. STRATEGICZNE PRIORYTETY I DZIAŁANIA

UE powinna chronić środowisko internetowe, w którym z korzyścią dla wszystkich zapewnione są wszystkie możliwe swobody oraz bezpieczeństwo. Uznając, że rozwiązywanie problemów związanych z bezpieczeństwem w cyberprzestrzeni to przede wszystkim zadanie państw członkowskich, w niniejszej strategii zaproponowano konkretne działania, które mogą poprawić ogólne wyniki UE. Działania te mają charakter długo- lub krótkoterminowy, obejmują one szereg instrumentów polityki[7] i wymagają udziału różnych rodzajów podmiotów, takich jak instytucje UE, państwa członkowskie i przedstawiciele branży.

Unijna wizja przedstawiona w niniejszej strategii składa się z pięciu strategicznych priorytetów, które uwzględniają wyzwania wymienione powyżej:

- Osiągnięcie odporności na zagrożenia cybernetyczne
- Radykalne ograniczenie cyberprzestępczości
- Opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO)
- Rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego
- Ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE

2.1. Osiągnięcie odporności na zagrożenia cybernetyczne

Aby zwiększać odporność w dziedzinie bezpieczeństwa cybernetycznego w UE, zarówno organy publiczne, jak i sektor prywatny muszą rozwijać zdolności i skutecznie współpracować. W oparciu o pozytywne wyniki osiągnięte w ramach przeprowadzonych do tej pory działań[8] dalsze inicjatywy na poziomie UE mogą w szczególności pomóc w przeciwdziałaniu zagrożeniom cybernetycznym o charakterze transgranicznym oraz w reagowaniu w skoordynowany sposób w sytuacjach awaryjnych. Działania te będą zdecydowanie wspierać sprawne funkcjonowanie rynku wewnętrznego i zwiększą bezpieczeństwo wewnętrzne w UE.

W przypadku niepodjęcia znaczących działań mających na celu poprawę zdolności, zwiększenie zasobów i usprawnienie procedur wykorzystywanych przez podmioty publiczne i prywatne w celu zapobiegania incydentom w zakresie bezpieczeństwa cybernetycznego, wykrywania ich oraz postępowania w przypadku ich wystąpienia, Europa pozostanie osłabiona. Dlatego też Komisja opracowała politykę dotyczącą bezpieczeństwa sieci i informacji (ang. *Network and Information Security*, NIS)[9]. W 2004 r. ustanowiono

---

[7] Działania związane z wymianą informacji w sytuacji, gdy w grę wchodzą dane osobowe, powinny być zgodne z unijnymi przepisami dotyczącymi ochrony danych.

[8] Zob. odniesienia w niniejszym komunikacie, jak również w dokumencie roboczym służb Komisji zawierającym ocenę skutków towarzyszącym wnioskowi Komisji w sprawie dyrektywy dotyczącej bezpieczeństwa sieci i informacji, w szczególności w pkt 4.1.4, 5.2 oraz w załącznikach 2, 6 i 8.

[9] W 2001 r. Komisja przyjęła komunikat pt. „Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia" (COM(2001) 298); w 2006 r. Komisja przyjęła strategię na rzecz

Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA)[10], a w chwili obecnej Rada i Parlament prowadzą negocjacje dotyczące nowego rozporządzenia w sprawie wzmocnienia i unowocześnienia jej mandatu[11]. Ponadto dyrektywa ramowa w sprawie usług łączności elektronicznej[12] nakłada na dostawców usług łączności elektronicznej obowiązek odpowiedniego przeciwdziałania zagrożeniom dotyczącym ich sieci i zgłaszania przypadków poważnych naruszeń bezpieczeństwa. Ponadto przepisy UE dotyczące ochrony danych[13] wymagają od administratorów danych wprowadzenia wymogów i zabezpieczeń w zakresie ochrony danych, w tym środków dotyczących bezpieczeństwa, natomiast w dziedzinie publicznie dostępnych usług łączności elektronicznej administratorzy danych zobowiązani są do zgłaszania właściwym organom krajowym incydentów powodujących naruszenie danych osobowych.

Pomimo postępów osiągniętych w oparciu o dobrowolne zobowiązania, wciąż istnieją braki w całej UE, zwłaszcza w zakresie zdolności krajowych, możliwości koordynacji w przypadku incydentów obejmujących więcej niż jedno państwo, jak również pod względem zaangażowania i gotowości sektora prywatnego. Niniejszej strategii towarzyszy wniosek dotyczący aktu prawnego, który m.in.:

- ustanawia wspólne minimalne wymogi w zakresie bezpieczeństwa sieci i informacji na poziomie krajowym, które zobowiązują państwa członkowskie do: wyznaczenia właściwych organów krajowych ds. bezpieczeństwa sieci i informacji, ustanowienia sprawnie funkcjonujących CERT oraz do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i informacji i krajowego planu współpracy w zakresie bezpieczeństwa sieci i informacji. Budowanie zdolności i koordynacja dotyczą także instytucji UE: w 2012 r. ustanowiono stały zespół reagowania na incydenty komputerowe odpowiedzialny za bezpieczeństwo systemów informatycznych instytucji, agencji i organów UE („CERT-UE”);
- ustanawia skoordynowane mechanizmy zapobiegania incydentom, wykrywania i ograniczania ich oraz reagowania na nie, które umożliwiają wymianę informacji i wzajemną pomoc między właściwymi organami krajowymi ds. bezpieczeństwa sieci i informacji. Właściwe organy krajowe ds. bezpieczeństwa sieci i informacji zostaną poproszone o zapewnienie właściwej współpracy obejmującej całą UE, w szczególności na podstawie unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji, który ma służyć do reagowania na incydenty cybernetyczne o wymiarze transgranicznym. Współpraca ta będzie również opierać się na wynikach prac europejskiego forum państw członkowskich (EFMS)[14], w ramach którego przeprowadzono konstruktywne rozmowy i wymianę doświadczeń dotyczących polityki publicznej w zakresie bezpieczeństwa sieci i informacji i które może stać się elementem mechanizmu współpracy po jego wejściu w życie.

---

bezpiecznego społeczeństwa informacyjnego (COM(2006) 251). W okresie od 2009 r. Komisja przyjęła również plan działania i komunikat w sprawie ochrony krytycznej infrastruktury informatycznej (CIIP) (COM(2009) 149, zatwierdzony rezolucją Rady 2009/C 321/01, oraz COM(2011) 163, zatwierdzony w konkluzjach Rady 10299/11).

10 Rozporządzenie (WE) nr 460/2004.

11 COM(2010) 521. Działania zaproponowane w niniejszej strategii nie pociągają za sobą konieczności zmiany bieżącego lub przyszłego mandatu ENISA.

12 Art. 13a i art. 13b dyrektywy 2002/21/WE.

13 Art. 17 dyrektywy 95/46/WE; art. 4 dyrektywy 2002/58/WE.

14 Europejskie forum państw członkowskich zostało utworzone na podstawie dokumentu COM(2009) 149 jako platforma dla władz publicznych państw członkowskich służąca do przeprowadzania rozmów na temat dobrych praktyk w zakresie bezpieczeństwa i odporności krytycznej infrastruktury informatycznej.

- zwiększa gotowość i zaangażowanie sektora prywatnego. Ponieważ przeważająca większość sieci i systemów informatycznych jest własnością prywatną i jest eksploatowana przez podmioty prywatne, silniejsze włączenie sektora prywatnego w działania na rzecz zwiększenia bezpieczeństwa cybernetycznego ma zasadnicze znaczenie. Sektor prywatny powinien opracować na poziomie technicznym swoje własne zdolności w zakresie odporności cybernetycznej i powinien zapewnić wymianę najlepszych praktyk między poszczególnymi branżami. Z opracowanych przez branżę instrumentów reagowania na incydenty, identyfikowania przyczyn i prowadzenia analiz kryminalistycznych powinien również korzystać sektor publiczny.

W przypadku podmiotów prywatnych nadal brakuje jednak skutecznych zachęt do dostarczania wiarygodnych danych na temat incydentów w zakresie bezpieczeństwa sieci i informacji oraz ich skutków, do systemowego przeciwdziałania zagrożeniom i do inwestowania w rozwiązania w dziedzinie bezpieczeństwa. Celem zaproponowanego aktu prawnego jest zatem doprowadzenie do sytuacji, w której podmioty działające w wielu kluczowych dziedzinach (energetyka, transport, bankowość, giełdy papierów wartościowych, technologie umożliwiające świadczenie kluczowych usług internetowych, a także organy administracji publicznej) dokonują oceny zagrożeń dla bezpieczeństwa cybernetycznego, na jakie są narażone, zapewniają niezawodność i odporność sieci i systemów informatycznych przy użyciu odpowiednich strategii przeciwdziałania zagrożeniom oraz wymieniają się informacjami z właściwymi organami ds. bezpieczeństwa sieci i informacji. Systemowe przeciwdziałanie zagrożeniom w zakresie bezpieczeństwa cybernetycznego może przyczynić się do zwiększenia możliwości gospodarczych i konkurencyjności w sektorze prywatnym, czyniąc bezpieczeństwo cybernetyczne jednym z atutów oferowanych usług.

Podmioty te będą zobowiązane do zgłaszania właściwym organom krajowym ds. bezpieczeństwa sieci i informacji incydentów mających znaczący wpływ na ciągłość podstawowych usług i na dostawy towarów uzależnione od sieci i systemów informatycznych.

Krajowe organy ds. bezpieczeństwa sieci i informacji powinny współpracować i wymieniać się informacjami z innymi organami regulacyjnymi, w szczególności z organami ochrony danych osobowych. Właściwe organy ds. bezpieczeństwa sieci i informacji powinny również zgłaszać organom ścigania poważne incydenty, które mogą mieć charakter przestępczy. Właściwe organy krajowe powinny również regularnie publikować na specjalnej stronie internetowej nieobjęte klauzulą tajności informacje na temat aktualnych wczesnych ostrzeżeń dotyczących incydentów i zagrożeń oraz skoordynowanych reakcji. Zobowiązania prawne nie powinny zastępować ani też uniemożliwiać prowadzenia nieformalnej oraz dobrowolnej współpracy, w tym między sektorem publicznym i prywatnym, mającej na celu zwiększenie poziomu bezpieczeństwa i wymianę informacji oraz najlepszych praktyk. Szczególnie ważną i przydatną platformą na poziomie UE, którą należy rozwijać, jest europejskie partnerstwo publiczno-prywatne na rzecz odporności (EP3R[15]).

[15] Europejskie partnerstwo publiczno-prywatne na rzecz odporności zostało zainicjowane na podstawie dokumentu COM(2009) 149. Platforma ta zainicjowała działania i intensywniejszą współpracę między sektorem publicznym i sektorem prywatnym w zakresie identyfikacji kluczowych zasobów, środków, funkcji i podstawowych wymogów w odniesieniu do odporności, jak również zapotrzebowania na współpracę i mechanizmy reagowania na zakrojone na szeroką skalę zakłócenia łączności elektronicznej.

Instrument „Łącząc Europę” (CEF)[16] zapewni wsparcie finansowe dla kluczowej infrastruktury, łącząc zdolności państw członkowskich w zakresie bezpieczeństwa sieci i informacji, a tym samym ułatwiając współpracę w całej UE.

Ponadto w celu rozwijania współpracy między państwami członkowskimi a sektorem prywatnym konieczne jest przeprowadzanie ćwiczeń w zakresie bezpieczeństwa cybernetycznego na poziomie UE. Pierwsze ćwiczenia z udziałem państw członkowskich przeprowadzono w 2010 r. („Cyber Europe 2010”), a drugie, również z udziałem sektora prywatnego, miały miejsce w październiku 2012 r. („Cyber Europe 2012”). W listopadzie 2011 r. przeprowadzono ćwiczenia symulacyjne z udziałem UE i USA („Cyber Atlantic 2011”). W nadchodzących latach planowane są dalsze ćwiczenia, w tym z partnerami międzynarodowymi.

Komisja:

- będzie kontynuować swoje działania, prowadzone przez Wspólne Centrum Badawcze (JRC) w ścisłej współpracy z władzami państw członkowskich oraz z właścicielami i operatorami infrastruktury krytycznej, obejmujące określanie słabych punktów europejskiej infrastruktury krytycznej pod względem bezpieczeństwa sieci i informacji oraz wspieranie rozwoju odpornych systemów;
- zainicjuje uruchomienie na początku 2013 r. pilotażowego projektu finansowanego przez UE[17], dotyczącego zwalczania botnetów i złośliwego oprogramowania, mającego na celu zapewnienie ram koordynacji i współpracy między państwami członkowskimi UE, organizacjami sektora prywatnego, takimi jak np. dostawcy usług internetowych, oraz partnerami międzynarodowymi.

Komisja zwraca się do ENISA o:

- zapewnienie państwom członkowskim pomocy przy budowaniu krajowych zdolności w zakresie bezpieczeństwa cybernetycznego, zwłaszcza poprzez rozwój wiedzy specjalistycznej w zakresie bezpieczeństwa i odporności przemysłowych systemów sterowania oraz infrastruktury transportowej i energetycznej;
- przeanalizowanie w 2013 r. wykonalności ustanowienia zespołu (zespołów) reagowania na komputerowe incydenty naruszające bezpieczeństwo dla przemysłowych systemów sterowania (ICS-CSIRT) w UE;
- dalsze wspieranie państw członkowskich i instytucji UE w przeprowadzaniu regularnych ogólnoeuropejskich ćwiczeń w zakresie bezpieczeństwa cybernetycznego, które będą również stanowić podstawę operacyjną udziału UE w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa cybernetycznego.

Komisja zwraca się do Parlamentu Europejskiego i Rady o:

- szybkie przyjęcie wniosku dotyczącego dyrektywy w sprawie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w całej Unii, który reguluje kwestie krajowych zdolności i krajowej gotowości, współpracy na poziomie UE

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. „Łącząc Europę” - pozycja budżetowa 09.03.02 – sieci telekomunikacyjne (wspieranie wzajemnych połączeń i interoperacyjności krajowych usług publicznych świadczonych online, a także dostępu do takich sieci).

[17] CIP-ICT PSP-2012-6, 325188. Budżet projektu to 15 mln EUR, a dofinansowanie ze strony UE wynosi 7,7 mln EUR.

oraz stosowania praktyk w zakresie przeciwdziałania zagrożeniom i wymiany informacji dotyczących bezpieczeństwa sieci i informacji.

Komisja zwraca się do przedstawicieli branży o:

- odegranie wiodącej roli w realizowaniu inwestycji na rzecz wysokiego poziomu bezpieczeństwa cybernetycznego i w opracowywaniu najlepszych praktyk i metod wymiany informacji na poziomie sektorowym i z organami publicznymi w celu zapewnienia silnej i skutecznej ochrony aktywów i osób, w szczególności poprzez partnerstwa publiczno-prywatne, takie jak EP3R i Trust in Digital Life (TDL)[18].

Działania informacyjne

Zapewnienie bezpieczeństwa cybernetycznego jest wspólnym obowiązkiem różnych podmiotów. Użytkownicy końcowi odgrywają kluczową rolę w zapewnianiu bezpieczeństwa sieci i informacji: muszą oni być świadomi zagrożeń, na jakie są narażeni w internecie, i muszą mieć możliwość podjęcia prostych kroków w celu obrony przed nimi.

W ostatnich latach opracowano kilka inicjatyw, które należy kontynuować. W działalność informacyjną zaangażowana jest zwłaszcza ENISA, która publikuje sprawozdania, organizuje specjalistyczne warsztaty oraz dba o rozwój partnerstw publiczno-prywatnych. Europol, Eurojust i krajowe organy ochrony danych również aktywnie prowadzą działania informacyjne. W październiku 2012 r. ENISA wraz z kilkoma państwami członkowskimi zorganizowała pilotażowy „Europejski miesiąc bezpieczeństwa cybernetycznego". Działania informacyjne są jednym z obszarów będących przedmiotem działalności grupy roboczej UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości[19], i są również istotne w kontekście programu „Bezpieczniejszy Internet"[20] (który dotyczy bezpieczeństwa dzieci w internecie).

Komisja zwraca się do ENISA o:

- przedstawienie w 2013 r. planu działania na rzecz wprowadzenia „prawa jazdy w dziedzinie bezpieczeństwa sieci i informacji", które stanowiłoby dobrowolny system certyfikacji i wspierałoby tym samym rozwój umiejętności i kompetencji informatyków (np. administratorów stron internetowych).

Komisja:

- zorganizuje w 2014 r., przy wsparciu ENISA, konkurs w dziedzinie bezpieczeństwa cybernetycznego, w trakcie którego studenci będą między sobą konkurować, proponując rozwiązania w zakresie bezpieczeństwa sieci i

---

18 http://www.trustindigitallife.eu/.

19 Zadaniem tej grupy roboczej, ustanowionej na szczycie UE-USA w listopadzie 2010 r. (MEMO/10/597), jest opracowanie opartych na współpracy strategii w odniesieniu do szeregu kwestii związanych z bezpieczeństwem cybernetycznym i cyberprzestępczością.

20 W ramach programu „Bezpieczniejszy Internet" finansowana jest sieć organizacji pozarządowych działających na rzecz bezpieczeństwa dzieci w internecie, sieć organów egzekwowania prawa, które wymieniają się informacjami i najlepszymi praktykami dotyczącymi zwalczania wykorzystywania internetu do celów rozpowszechniania materiałów związanych z seksualnym wykorzystywaniem dzieci oraz sieć naukowców, którzy gromadzą informacje na temat zastosowań technologii internetowych w życiu dzieci, zagrożeń związanych z tymi technologiami oraz konsekwencji ich stosowania.

informacji.

Komisja wzywa państwa członkowskie[21] do:

- organizowania co roku od 2013 r. miesiąca bezpieczeństwa cybernetycznego, przy wsparciu ENISA i z udziałem sektora prywatnego, w celu poszerzenia wiedzy na ten temat wśród użytkowników końcowych. Od 2014 r. miesiąc bezpieczeństwa cybernetycznego będzie organizowany jednocześnie w UE i w USA;
- zintensyfikowania działań krajowych w dziedzinie edukacji i szkoleń związanych z bezpieczeństwem sieci i informacji, poprzez wprowadzenie szkoleń w zakresie bezpieczeństwa sieci i informacji w szkołach do 2014 r., szkoleń dla studentów informatyki w zakresie bezpieczeństwa sieci i informacji, bezpiecznego oprogramowania oraz ochrony danych osobowych oraz podstawowych szkoleń w zakresie bezpieczeństwa sieci i informacji dla pracowników administracji publicznej.

Komisja zwraca się do przedstawicieli branży o:

- prowadzenie działań informacyjnych dotyczących bezpieczeństwa cybernetycznego na wszystkich poziomach, zarówno w ramach stosowanych praktyk gospodarczych, jak i w relacjach z klientami. Przedstawiciele przemysłu powinni zwrócić szczególną uwagę na to, w jaki sposób doprowadzić do sytuacji, w której dyrektorzy generalni i zarządy będą ponosić większą odpowiedzialność za zapewnienie bezpieczeństwa cybernetycznego.

2.2. Radykalne ograniczenie cyberprzestępczości

Im większa część naszego życia toczy się w świecie cyfrowym, tym więcej stwarzamy cyberprzestępcom okazji do popełniania przestępstw. Cyberprzestępczość jest jedną z najszybciej rosnących form przestępczości – codziennie pada jej ofiarą ponad milion ludzi na całym świecie. Cyberprzestępcy i sieci cyberprzestępcze stają się coraz bardziej wyrafinowane i w związku z tym musimy mieć właściwe narzędzia i zdolności operacyjne, aby móc stawić im czoła. Cyberprzestępczość jest bardzo rentowna i wiąże się z niewielkim ryzykiem, a przestępcy często wykorzystują anonimowe domeny internetowe. Cyberprzestępczość nie zna granic – globalny zasięg internetu oznacza, że egzekwując prawo, należy przyjąć skoordynowane i wspólne podejście ponadgraniczne, aby właściwie reagować na to rosnące zagrożenie.

Rygorystyczne i skuteczne przepisy

UE i państwa członkowskie potrzebują rygorystycznych i skutecznych przepisów w celu zwalczania cyberprzestępczości. Konwencja Rady Europy o cyberprzestępczości, znana również jako konwencja budapeszteńska, jest wiążącym traktatem międzynarodowym, który stanowi skuteczne ramy dla przepisów prawa krajowego.

[21] Również przy udziale właściwych organów krajowych, w tym organów ds. bezpieczeństwa sieci i informacji oraz organów ochrony danych.

UE przyjęła już przepisy dotyczące cyberprzestępczości, w tym dyrektywę w sprawie zwalczania wykorzystywania seksualnego dzieci w internecie oraz pornografii dziecięcej[22]. UE jest również bliska porozumienia w sprawie dyrektywy w sprawie ataków na systemy informatyczne, w szczególności poprzez wykorzystanie botnetów.

Komisja:

- zapewni szybką transpozycję i wdrożenie dyrektyw dotyczących cyberprzestępczości;
- wezwie te państwa członkowskie, które nie ratyfikowały jeszcze **konwencji Rady Europy o cyberprzestępczości**, do jej jak najszybszego ratyfikowania i do wdrożenia jej postanowień.

Zwiększenie zdolności operacyjnej w celu zwalczania cyberprzestępczości

Rozwój technik stosowanych w cyberprzestępczości jest coraz szybszy. Jednocześnie organy ścigania nie są w stanie zwalczać cyberprzestępczości przy użyciu przestarzałych narzędzi operacyjnych. Obecnie nie wszystkie państwa członkowskie UE posiadają zdolności operacyjne, których potrzebują, aby skutecznie reagować na zagrożenia związane z cyberprzestępczością. Wszystkie państwa członkowskie potrzebują skutecznych krajowych jednostek ścigania cyberprzestępczości.

Komisja:

- będzie wspierać państwa członkowskie, poprzez swoje programy finansowania[23], w **identyfikowaniu braków i zwiększaniu zdolności** w zakresie prowadzenia dochodzeń i zwalczania cyberprzestępczości; Komisja będzie ponadto wspierać organy, które zapewniają kontakty między środowiskiem naukowym/akademickim, podmiotami odpowiedzialnymi za egzekwowanie prawa i sektorem prywatnym, tak jak ma to miejsce w przypadku prac prowadzonych przez finansowane przez Komisję centra doskonałości zajmujące się cyberprzestępczością utworzone już w niektórych państwach członkowskich;
- będzie koordynować – wraz z państwami członkowskimi – działania mające na celu określenie najlepszych praktyk i najlepszych dostępnych technik zwalczania cyberprzestępczości (np. w odniesieniu do rozwoju i wykorzystywania narzędzi analizy kryminalistycznej lub analizy zagrożeń), w tym również przy wsparciu JRC;
- będzie ściśle współpracować z utworzonym niedawno w ramach **Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3)** oraz z **Eurojustem** w celu dostosowania rozwiązań politycznych do najlepszych praktyk z punktu widzenia operacyjnego.

[22] Dyrektywa 2011/93/UE zastępująca decyzję ramową Rady 2004/68/WSiSW.

[23] W 2013 r. – w ramach programu „ Zapobieganie i walka z przestępczością" (ISEC). Po 2013 r. – w ramach Funduszu Bezpieczeństwa Wewnętrznego (nowy instrument w ramach wieloletnich ram finansowych).

Usprawniona koordynacja na poziomie UE

UE może uzupełniać działania państw członkowskich poprzez ułatwienie przyjęcia skoordynowanego i opartego na współpracy podejścia, skupiającego organy ścigania i organy sądowe oraz zainteresowane podmioty z sektora publicznego i prywatnego z UE i spoza jej granic.

Komisja:

- będzie wspierać utworzone niedawno Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), będące centralnym europejskim punktem kontaktowym ds. zwalczania cyberprzestępczości. EC3 będzie dostarczać analizy i dane, wspierać dochodzenia, zapewniać wysokiej jakości analizę kryminalistyczną, ułatwiać współpracę, tworzyć kanały wymiany informacji między właściwymi organami w państwach członkowskich, sektorem prywatnym i innymi zainteresowanymi stronami, a także będzie stopniowo służyć jako głos organów ścigania[24];
- będzie wspierać działania mające na celu zwiększenie odpowiedzialności rejestratorów nazw domen oraz zapewnienie dokładności informacji dotyczących właścicieli stron internetowych, w szczególności na podstawie zaleceń dotyczących egzekwowania prawa wydanych przez Internetową Korporację ds. Nadawania Nazw i Numerów (ICANN), zgodnie z prawem unijnym, w tym zgodnie z przepisami dotyczącymi ochrony danych;
- będzie kontynuować działania UE mające na celu zwalczanie wykorzystywania seksualnego dzieci w internecie, opierając się na przyjętych niedawno aktach prawnych. Komisja przyjęła europejską strategię na rzecz lepszego internetu dla dzieci[25] oraz wraz z państwami z UE i spoza UE zainicjowała działalność **światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w internecie w celach seksualnych**[26]. Sojusz jest motorem dalszych działań podejmowanych przez państwa członkowskie przy wsparciu Komisji i EC3.

Komisja zwraca się do Europolu (EC3) o:

- udzielenie państwom członkowskim w fazie początkowej wsparcia analitycznego i operacyjnego w prowadzeniu dochodzeń dotyczących cyberprzestępstw, tak aby pomóc im w rozbiciu i zakłóceniu działalności sieci cyberprzestępczych działających głównie w obszarach wykorzystywania seksualnego dzieci, oszustw płatniczych, botnetów i złośliwych ataków;
- regularne publikowanie sprawozdań strategicznych i operacyjnych na temat tendencji i pojawiających się zagrożeń w celu określenia priorytetów oraz celów dochodzeń prowadzonych przez zespoły ds. cyberprzestępczości w państwach członkowskich.

[24] W dniu 28 marca 2012 r. Komisja Europejska przyjęła komunikat pt. „Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością".

[25] COM(2012) 196 final.

[26] Konkluzje Rady w sprawie światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w internecie w celach seksualnych (wspólne oświadczenie UE i USA) z dnia 7 i 8 czerwca 2012 r. oraz deklaracja w sprawie utworzenia światowego sojuszu przeciwko niegodziwemu traktowaniu dzieci w internecie (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

Komisja wzywa Europejskie Kolegium Policyjne (CEPOL), aby we współpracy z Europolem:

- koordynowało przygotowywanie i planowanie szkoleń w celu zapewnienia organom ścigania wiedzy i doświadczenia niezbędnych do skutecznej walki z cyberprzestępczością.

Komisja zwraca się do Eurojustu o:

- określenie głównych przeszkód utrudniających współpracę sądową przy dochodzeniach w sprawie cyberprzestępstw oraz utrudniających koordynację między państwami członkowskimi i państwami trzecimi, a także zwraca się o wsparcie dochodzeń i ścigania cyberprzestępczości, zarówno na poziomie operacyjnym, jak i poziomie strategicznym, jak również o wsparcie działalności szkoleniowej w tej dziedzinie.

Komisja zwraca się do Eurojustu i Europolu (EC3) o:

- podjęcie ścisłej współpracy, między innymi poprzez wymianę informacji, w celu zwiększenia ich skuteczności w zwalczaniu cyberprzestępczości, zgodnie z ich odpowiednimi mandatami i kompetencjami.
-

2.3. Opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO)

Działania na rzecz bezpieczeństwa cybernetycznego w UE mogą również dotyczyć obrony cybernetycznej. W celu zwiększenia odporności systemów łączności i systemów informatycznych, od których uzależnione są interesy państw członkowskich w dziedzinie obronności i bezpieczeństwa narodowego, rozwój zdolności w zakresie obrony cybernetycznej powinien koncentrować się wykrywaniu, reagowaniu i usuwaniu skutków w przypadku wystąpienia zaawansowanych technologicznie zagrożeń cybernetycznych.

Mając na uwadze, że zagrożenia są wielowymiarowe, należy wykorzystywać synergie między cywilnymi i wojskowymi koncepcjami dotyczącymi ochrony krytycznych zasobów cybernetycznych. Działania te powinny być wspierane przez prace badawczo-rozwojowe, jak również przez bliższą współpracę między rządami, sektorem prywatnym i środowiskiem akademickim w UE. Aby uniknąć powielania działań, UE będzie analizować możliwości dotyczące tego, w jaki sposób UE i NATO mogą uzupełniać swoje działania w celu zwiększenia odporności krytycznej infrastruktury rządowej, obronnej i innych rodzajów infrastruktury informatycznej, od której uzależnieni są członkowie obu organizacji.

Wysoki Przedstawiciel zaprosi państwa członkowskie i Europejską Agencję Obrony do współpracy i będzie się koncentrować się na następujących kluczowych działaniach:

- ocena wymogów operacyjnych w zakresie obrony cybernetycznej w UE oraz wspieranie rozwoju unijnych zdolności i technologii w zakresie obrony cybernetycznej w celu uwzględnienia wszystkich aspektów rozwoju zdolności, w tym doktryn, metod zarządzania, organizacji, personelu, szkoleń, technologii, infrastruktury, logistyki i interoperacyjności;

- opracowanie ram politycznych dla obrony cybernetycznej w UE w celu zapewnienia ochrony sieci w ramach misji i operacji WPBiO, w tym opracowanie dynamicznych metod przeciwdziałania zagrożeniom, poprawa analizy zagrożeń i wymiana informacji. Zwiększenie możliwości korzystania ze szkoleń i ćwiczeń w zakresie obrony cybernetycznej przez personel wojskowy w kontekście europejskim i wielonarodowym, w tym włączenie elementów obrony cybernetycznej do bieżących katalogów szkoleń;

- promowanie dialogu i koordynacji pomiędzy podmiotami cywilnymi i wojskowymi w UE, kładąc szczególny nacisk na wymianę dobrych praktyk, wymianę informacji, wczesne ostrzeżenia, reagowanie na incydenty, ocenę zagrożeń, działania informacyjne oraz na uznanie bezpieczeństwa cybernetycznego za priorytet;

- zapewnianie dialogu z partnerami międzynarodowymi, w tym z NATO, oraz z innymi organizacjami międzynarodowymi i wielonarodowymi centrami doskonałości, aby zapewnić skuteczne zdolności obronne, określić obszary współpracy i uniknąć powielania wysiłków.

2.4. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego

Europa posiada doskonałe możliwości badawcze i rozwojowe, ale wielu światowych liderów dostarczających innowacyjne produkty i usługi w zakresie technologii informacyjno-komunikacyjnych (ICT) znajduje się poza UE. Istnieje ryzyko, że Europa staje się nadmiernie uzależniona nie tylko od ICT pochodzących z zewnątrz, ale również od rozwiązań w zakresie bezpieczeństwa opracowanych poza jej granicami. Należy zagwarantować, aby elementy sprzętu i oprogramowania produkowane w UE oraz w państwach trzecich, które są stosowane w kluczowych usługach i w kluczowej infrastrukturze oraz w coraz większym stopniu w urządzeniach przenośnych, były wiarygodne i bezpieczne oraz aby gwarantowały ochronę danych osobowych.

Wspieranie jednolitego rynku produktów związanych z bezpieczeństwem cybernetycznym

Wysoki poziom bezpieczeństwa można zapewnić jedynie wtedy, gdy wszystkie podmioty w łańcuchu wartości (np. producenci urządzeń, twórcy oprogramowania, dostawcy usług społeczeństwa informacyjnego) traktują zapewnienie bezpieczeństwa jako kwestię priorytetową. Wydaje się jednak[27], iż wiele podmiotów nadal uznaje konieczność zapewnienia bezpieczeństwa jedynie za dodatkowe obciążenie, przez co zapotrzebowanie na rozwiązania w zakresie bezpieczeństwa jest ograniczone. Konieczne jest zatem wprowadzenie stosownych wymogów dotyczących bezpieczeństwa cybernetycznego w całym łańcuchu

[27] Zob. dokument roboczy służb Komisji zawierający ocenę skutków towarzyszący wnioskowi Komisji w sprawie dyrektywy dotyczącej bezpieczeństwa sieci i informacji, ppkt 4.1.5.2.

wartości w odniesieniu do produktów ICT wykorzystywanych w Europie. Sektor prywatny potrzebuje zachęt, aby zapewnić wysoki poziom bezpieczeństwa cybernetycznego. Przykładowo, etykiety potwierdzające właściwy poziom bezpieczeństwa cybernetycznego umożliwią przedsiębiorstwom osiągającym dobre wyniki w tym zakresie wykorzystanie tej informacji jako atutu, który da im przewagę konkurencyjną. Ponadto wprowadzenie obowiązków określonych we wniosku dotyczącym dyrektywy w sprawie bezpieczeństwa sieci i informacji znacząco przyczyniłoby się do zwiększenia konkurencyjności przedsiębiorstw podlegającym tym obowiązkom.

Należy również stymulować ogólnoeuropejski popyt rynkowy na produkty o wysokim poziomie bezpieczeństwa. Po pierwsze, niniejsza strategia ma na celu zwiększenie współpracy i przejrzystości w zakresie bezpieczeństwa produktów ICT. Wzywa ona do utworzenia platformy skupiającej zainteresowane strony z sektorów publicznego i prywatnego w Europie w celu określenia dobrych praktyk dotyczących bezpieczeństwa cybernetycznego w całym łańcuchu wartości i w celu stworzenia korzystnych warunków rynkowych dla rozwoju i przyjmowania bezpiecznych rozwiązań ICT. Głównym celem powinno być stworzenie zachęt do wprowadzania odpowiednich strategii przeciwdziałania zagrożeniom oraz do przyjmowania norm i rozwiązań w zakresie bezpieczeństwa, jak również do ewentualnego ustanowienia dobrowolnych ogólnounijnych systemów certyfikacji opartych na systemach istniejących już w UE i na arenie międzynarodowej. Komisja będzie wspierać przyjmowanie spójnych strategii wśród państw członkowskich, aby uniknąć rozbieżności mogących powodować dla przedsiębiorstw niedogodności płynące z lokalizacji.

Po drugie, Komisja będzie wspierać opracowanie norm bezpieczeństwa i zapewni pomoc przy tworzeniu ogólnounijnych dobrowolnych systemów certyfikacji w dziedzinie chmury obliczeniowej, uwzględniając przy tym odpowiednio konieczność zapewnienia ochrony danych. Prace powinny się koncentrować na bezpieczeństwie łańcucha dostaw, w szczególności w krytycznych sektorach gospodarki (przemysłowe systemy sterowania, infrastruktura energetyczna i transportowa). Prace te powinny się opierać na pracach normalizacyjnych prowadzonych przez europejskie organizacje normalizacyjne (CEN, CENELEC i ETSI)[28] oraz grupę koordynacyjną ds. bezpieczeństwa cybernetycznego (CSCG), jak również na wiedzy specjalistycznej, jaką dysponują ENISA, Komisja i inne zainteresowane podmioty.

Komisja:

- uruchomi w 2013 r. platformę publiczno-prywatną dla rozwiązań w dziedzinie bezpieczeństwa sieci i informacji w celu stwarzania zachęt do przyjmowania bezpiecznych rozwiązań ICT i do powszechnego zapewniania wysokiego poziomu bezpieczeństwa cybernetycznego w odniesieniu do produktów ICT, które mają być wykorzystywane w Europie;
- przedstawi w 2014 r. zalecenia dotyczące zapewnienia bezpieczeństwa cybernetycznego w całym łańcuchu wartości ICT w oparciu o prace tej platformy;
- przeanalizuje, w jaki sposób główni dostawcy sprzętu i oprogramowania ICT mogliby informować właściwe organy krajowe o wykrytych słabych punktach, które mogą mieć znaczący wpływ na bezpieczeństwo.

[28] Zwłaszcza w ramach normy M/490 dotyczącej inteligentnych sieci w odniesieniu do pierwszego zestawu norm dla inteligentnych sieci i architektury referencyjnej.

Komisja zwraca się do ENISA o:

- opracowanie, we współpracy z właściwymi organami krajowymi, zainteresowanymi stronami, międzynarodowymi i europejskimi organami normalizacyjnymi i działającym przy Komisji Europejskiej Wspólnym Centrum Badawczym, wytycznych technicznych i zaleceń dotyczących przyjmowania norm i stosowania dobrych praktyk w zakresie bezpieczeństwa sieci i informacji w sektorze publicznym i prywatnym.

Komisja wzywa zainteresowane podmioty publiczne i prywatne do:

- stymulowania rozwoju i przyjmowania branżowych norm bezpieczeństwa, norm technicznych i zasad uwzględniania już na etapie projektowania funkcji służących ochronie bezpieczeństwa i prywatności przez producentów produktów ICT i dostawców usług ICT, w tym przez dostawców usług w zakresie chmury obliczeniowej. Oprogramowanie i sprzęt komputerowy nowej generacji należy wyposażać w silniejsze, wbudowane i przyjazne dla użytkownika elementy służące zapewnieniu bezpieczeństwa;
- opracowania branżowych norm dotyczących wyników osiąganych przez przedsiębiorstwa w zakresie bezpieczeństwa cybernetycznego oraz do poprawy informacji podawanych do wiadomości publicznej poprzez opracowanie etykiet bezpieczeństwa lub znaków typu „kite mark", które ułatwią konsumentom orientację na rynku.

Wspieranie inwestycji w badania i rozwój oraz innowacji

Badania i rozwój mogą stanowić podporę skutecznej i silnej polityki przemysłowej, wspierać wiarygodność branży ICT w Europie, usprawnić funkcjonowanie rynku wewnętrznego i zmniejszyć zależność Europy od zagranicznych technologii. Badania i rozwój powinny uzupełnić braki technologiczne w dziedzinie bezpieczeństwa ICT, zapewnić przygotowanie do walki z nowymi problemami w zakresie bezpieczeństwa, reagować na ciągłe zmiany potrzeb użytkowników i odnosić korzyści z technologii podwójnego zastosowania. W ramach badań i rozwoju należy również nadal wspierać rozwój kryptografii. Powyższe dążenia należy uzupełnić działaniami na rzecz lepszego przełożenia wyników badań i rozwoju na rozwiązania komercyjne poprzez stworzenie niezbędnych zachęt i wprowadzenie właściwych warunków politycznych.

UE powinna optymalnie wykorzystać program ramowy w zakresie badań naukowych i innowacji „Horyzont 2020"[29], który ma zostać uruchomiony w 2014 r. Wniosek Komisji zawiera konkretne cele dotyczące wiarygodności ICT oraz zwalczania cyberprzestępczości, które są zgodne z niniejszą strategią. Program „Horyzont 2020" będzie wspierać badania w dziedzinie bezpieczeństwa związane z nowymi technologiami ICT, dostarczać rozwiązania dla bezpiecznych systemów, usług i aplikacji ICT typu end-to-end, zapewniać odpowiednie zachęty do wdrażania i przyjmowania istniejących rozwiązań, oraz uwzględniać kwestię

[29] „Horyzont 2020" to instrument służący wdrażaniu „Unii innowacji" – jednej z inicjatyw przewodnich strategii „Europa 2020", która ma na celu zapewnienie konkurencyjności Europy w skali międzynarodowej. Od 2014 do 2020 r. ten nowy unijny program ramowy na rzecz badań naukowych i innowacji będzie częścią działań mających na celu osiągnięcie dodatkowego wzrostu gospodarczego i tworzenie nowych miejsc pracy w Europie.

interoperacyjności sieci i systemów informatycznych. Szczególny nacisk na poziomie UE położony zostanie na optymalizację i sprawniejszą koordynację różnych programów finansowania („Horyzont 2020", Fundusz Bezpieczeństwa Wewnętrznego, badania finansowane przez EAO, w tym europejskie ramy współpracy).

Komisja:

- wykorzysta „Horyzont 2020" do podjęcia różnych kwestii w dziedzinie ochrony prywatności i bezpieczeństwa związanych z ICT, począwszy od badań i rozwoju, aż po innowacje i wdrażanie. „Horyzont 2020" umożliwi również opracowanie narzędzi i instrumentów służących do walki z działalnością przestępczą i terrorystyczną wymierzoną w środowisko cybernetyczne;
- ustanowi mechanizmy skuteczniejszej koordynacji programów badawczych instytucji Unii Europejskiej i państw członkowskich oraz zachęci państwa członkowskie do zwiększenia nakładów na badania i rozwój.

Komisja wzywa państwa członkowskie do:

- opracowania do końca 2013 r. dobrych praktyk dotyczących wykorzystania **siły nabywczej administracji publicznych** (np. poprzez zamówienia publiczne) w celu wspierania rozwoju i wdrażania zabezpieczeń w produktach i usługach ICT;
- wspierania udziału, już na wczesnym etapie, przemysłu i środowiska akademickiego w opracowywaniu i koordynacji rozwiązań. Należy tego dokonać poprzez pełne wykorzystanie europejskiej bazy przemysłowej i powiązanych innowacji technologicznych osiągniętych dzięki pracom badawczo-rozwojowym oraz poprzez koordynację programów badawczych organizacji cywilnych i wojskowych.

Komisja zwraca się do Europolu i ENISA o:

- zidentyfikowanie pojawiających się tendencji i potrzeb w kontekście ewoluujących modeli cyberprzestępczości i bezpieczeństwa cybernetycznego, tak aby możliwe było opracowanie odpowiednich narzędzi i technologii służących do analizy kryminalistycznej.

Komisja wzywa zainteresowane podmioty publiczne i prywatne do:

- opracowania, we współpracy z sektorem ubezpieczeniowym, **zharmonizowanych metod pomiaru do celów obliczania premii z tytułu ryzyka**, dzięki czemu przedsiębiorstwa, które dokonały inwestycji w dziedzinie bezpieczeństwa, mogłyby korzystać z niższych premii z tytułu ryzyka.

2.5. Ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE

Utrzymanie wolnej, otwartej i chronionej cyberprzestrzeni jest wyzwaniem na skalę światową, któremu UE musi stawić czoła wraz z odpowiednimi partnerami i organizacjami międzynarodowymi, sektorem prywatnym i społeczeństwem obywatelskim.

W ramach swojej międzynarodowej polityki w zakresie cyberprzestrzeni UE będzie promować otwarty i wolny internet, wspierać działania mające na celu opracowanie norm zachowania oraz stosować w odniesieniu do cyberprzestrzeni istniejące już przepisy

międzynarodowe. UE będzie również działać na rzecz zlikwidowania przepaści cyfrowej oraz będzie aktywnie uczestniczyć w działaniach międzynarodowych zmierzających do budowy zdolności w zakresie bezpieczeństwa cybernetycznego. Zaangażowanie UE w kwestie bezpieczeństwa cybernetycznego na arenie międzynarodowej będzie zgodne z podstawowymi wartościami UE, takimi jak poszanowanie godności osoby ludzkiej, wolności, demokracji, równości i praworządności oraz poszanowanie praw podstawowych.

Włączanie kwestii dotyczących cyberprzestrzeni do polityki zewnętrznej UE oraz do wspólnej polityki zagranicznej i bezpieczeństwa

Komisja, Wysoki Przedstawiciel i państwa członkowskie powinny opracować spójną politykę międzynarodową UE dotyczącą cyberprzestrzeni, która będzie miała na celu zwiększenie zaangażowania i umocnienie relacji z kluczowymi partnerami i organizacjami międzynarodowymi, jak również z przedstawicielami społeczeństwa obywatelskiego i sektora prywatnego. Konsultacje UE z partnerami międzynarodowymi w dziedzinie cyberbezpieczeństwa powinny być planowane, koordynowane i realizowane w taki sposób, aby stanowiły wartość dodaną w stosunku do istniejących dwustronnych rozmów między państwami członkowskimi UE a państwami trzecimi. UE na nowo położy nacisk na dialog z państwami trzecimi, ze szczególnym uwzględnieniem podobnie myślących partnerów podzielających wartości UE. UE będzie działać na rzecz zapewnienia wysokiego poziomu ochrony danych, w tym podczas przekazywania danych osobowych do państw trzecich. Aby sprostać światowym wyzwaniom związanym z przestrzenią cybernetyczną, UE będzie dążyła do zacieśnienia współpracy z organizacjami działającymi w tej dziedzinie, takimi jak Rada Europy, OECD, ONZ, OBWE, NATO, Unia Afrykańska, ASEAN i OPA. Na poziomie stosunków dwustronnych szczególnie ważna jest współpraca ze Stanami Zjednoczonymi. Będzie ona dalej rozwijana, w szczególności w ramach grupy roboczej UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości.

Jednym z najważniejszych elementów międzynarodowej polityki UE w dziedzinie cyberbezpieczeństwa będzie promowanie cyberprzestrzeni jako obszaru, w którym panuje wolność i przestrzegane są prawa podstawowe. Rozszerzenie dostępu do internetu powinno przyczyniać się do przyspieszenia reform demokratycznych i ich wspierania na całym świecie. Rozwój globalnej infrastruktury komunikacyjnej nie powinien pociągać za sobą cenzury i masowej inwigilacji. UE powinna promować społeczną odpowiedzialność przedsiębiorstw[30] i powinna zainicjować międzynarodowe działania na rzecz poprawy globalnej koordynacji w tej dziedzinie.

Odpowiedzialność za zwiększenie bezpieczeństwa w cyberprzestrzeni spoczywa na wszystkich podmiotach tworzących globalne społeczeństwo informacyjne, począwszy od obywateli aż po administracje rządowe. UE wspiera działania mające na celu określenie norm zachowania w cyberprzestrzeni, do których powinny się stosować wszystkie zainteresowane strony. Podobnie jak UE oczekuje od obywateli przestrzegania norm obywatelskich i społecznych oraz przepisów prawa w internecie, tak samo państwa powinny stosować się do obowiązujących norm i przepisów. W kwestiach bezpieczeństwa międzynarodowego UE zachęca do wspierania działań służących budowaniu zaufania do bezpieczeństwa cybernetycznego, aby zwiększyć przejrzystość oraz zmniejszyć ryzyko powstania nieprawdziwych wyobrażeń o podejmowanych przez państwa działaniach.

[30] Odnowiona strategia UE na lata 2011-2014 dotycząca społecznej odpowiedzialności przedsiębiorstw, COM(2011) 681 final.

UE nie wzywa do utworzenia nowych międzynarodowych instrumentów prawnych dotyczących przestrzeni cybernetycznej.

Zobowiązania prawne zawarte w Międzynarodowym pakcie praw obywatelskich i politycznych, Europejskiej konwencji praw człowieka oraz Karcie praw podstawowych UE powinny być przestrzegane również w internecie. UE skoncentruje się na tym, w jaki sposób zapewnić egzekwowanie tych zobowiązań również w cyberprzestrzeni.

Jeśli chodzi o zwalczanie cyberprzestępczości, stosownym instrumentem jest konwencja budapeszteńska, która jest otwarta do przyjęcia przez państwa trzecie. Stanowi ona wzór dla ustawodawstwa krajowego w dziedzinie cyberprzestępczości i jest podstawą współpracy międzynarodowej w tej dziedzinie.

Jeżeli na cyberprzestrzeń rozszerzą się konflikty zbrojne, zastosowanie będzie mieć międzynarodowe prawo humanitarne oraz, w stosownych przypadkach, prawo praw człowieka.

Rozwój zdolności w zakresie bezpieczeństwa cybernetycznego i odporności infrastruktury informatycznej w państwach trzecich

Zacieśnienie współpracy międzynarodowej będzie mieć korzystny wpływ na sprawne funkcjonowanie infrastruktur bazowych, które umożliwiają i ułatwiają świadczenie usług telekomunikacyjnych. Współpraca taka obejmuje wymianę najlepszych praktyk, dzielenie się informacjami, wydawanie wczesnych ostrzeżeń, wspólne ćwiczenia w zakresie reagowania na incydenty itd. UE będzie prowadzić działania zmierzające do osiągnięcia tego celu polegające na intensyfikacji prowadzonych już działań międzynarodowych na rzecz wzmocnienia sieci współpracy w dziedzinie ochrony krytycznej infrastruktury informatycznej (CIIP), w ramach których współpracują administracje rządowe i sektor prywatny.

Nie wszystkie części świata odnoszą korzyści z internetu, ze względu na brak otwartego, bezpiecznego, interoperacyjnego i niezawodnego dostępu do tego zasobu. Unia Europejska będzie więc nadal wspierać działania państw, których celem jest poprawa dostępu do internetu dla swoich obywateli, zwiększenie możliwości wykorzystywania internetu, zapewnienie jego integralności i bezpieczeństwa oraz skuteczne zwalczanie cyberprzestępczości.

We współpracy z państwami członkowskimi Komisja oraz Wysoki Przedstawiciel:

- będą prowadzić działania mające na celu opracowanie spójnej międzynarodowej polityki UE dotyczącej cyberprzestrzeni na rzecz zwiększenia zaangażowania kluczowych partnerów i organizacji międzynarodowych, włączenie kwestii związanych z bezpieczeństwem cybernetycznym do głównego nurtu WPZiB oraz mające na celu poprawę koordynacji kwestii związanych z bezpieczeństwem cybernetycznym w skali światowej;
- będą wspierać rozwój norm zachowania oraz środków służących do zwiększenia zaufania do bezpieczeństwa cybernetycznego; będą ułatwiać rozmowy dotyczące tego, w jaki sposób stosować istniejące przepisy prawa międzynarodowego w odniesieniu do cyberprzestrzeni i w jaki sposób promować konwencję budapeszteńską w celu zwalczania cyberprzestępczości;

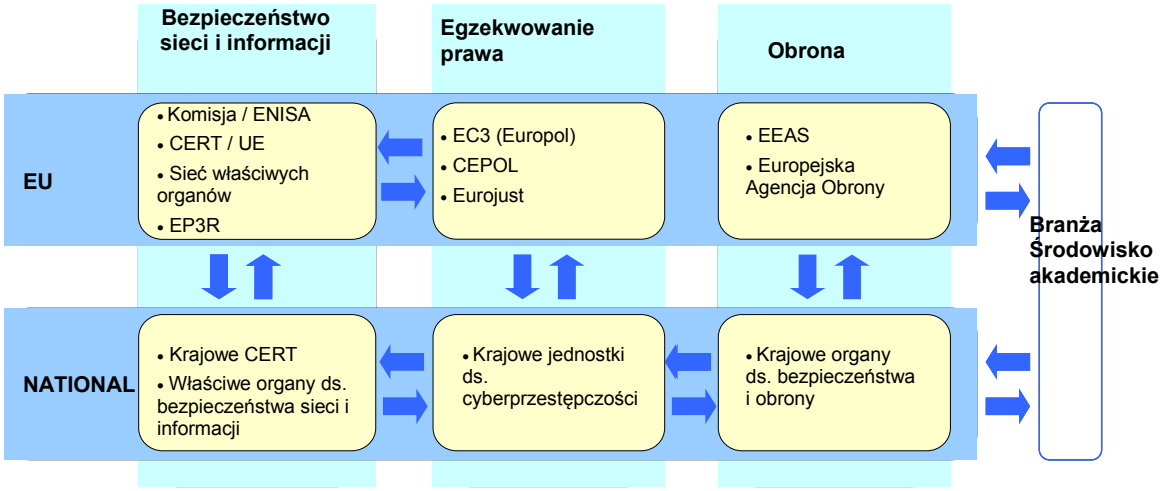
- będą wspierać propagowanie i ochronę praw podstawowych, w tym prawa do dostępu do informacji i wolności wypowiedzi, koncentrując się na: a) opracowaniu nowych publicznych wytycznych w sprawie wolności wypowiedzi w internecie i poza nim; b) monitorowaniu eksportu produktów lub usług, które mogłyby zostać wykorzystane do cenzurowania lub masowej inwigilacji w internecie; c) opracowaniu środków i narzędzi mających na celu zwiększenie dostępu do internetu oraz jego otwartości i odporności, tak aby możliwe było przeciwdziałanie cenzurze lub masowej inwigilacji przy pomocy technik teleinformatycznych; d) umożliwianiu zainteresowanym stronom stosowania technologii teleinformatycznych w celu propagowania praw podstawowych;
- będą współpracować z partnerami i organizacjami międzynarodowymi, sektorem prywatnym i społeczeństwem obywatelskim na rzecz rozwoju globalnych zdolności w państwach trzecich w celu poprawy dostępu do informacji oraz do otwartego internetu, zapobiegania zagrożeniom cybernetycznym i zwalczania ich, w tym zdarzeniom przypadkowym, cyberprzestępczości i cyberterroryzmowi, oraz w celu zapewnienia koordynacji działań darczyńców zmierzających do rozbudowy zdolności;
- będą wykorzystywać różne unijne instrumenty pomocowe w celu rozbudowy zdolności w zakresie bezpieczeństwa cybernetycznego, zapewniając m.in. pomoc w organizacji szkoleń poświęconych zwalczaniu zagrożeń cybernetycznych, skierowanych do organów ścigania, organów sądowych i personelu technicznego, jak również będą wspierać wprowadzanie odpowiednich krajowych polityk, strategii i instytucji w państwach trzecich;
- zwiększą koordynację polityki i wymianę informacji za pośrednictwem międzynarodowych sieci ochrony krytycznej infrastruktury informatycznej, takich jak np. sieć Meridian, oraz zintensyfikują współpracę między właściwymi organami ds. bezpieczeństwa sieci i informacji i innymi organami.

3. ROLE I OBOWIĄZKI

W uzależnionych od internetu gospodarce i społeczeństwie incydenty cybernetyczne nie zatrzymują się na granicach. Wszystkie podmioty, począwszy od właściwych organów ds. bezpieczeństwa sieci i informacji, poprzez CERT, organy ścigania i branżę, muszą wziąć na siebie odpowiedzialność za zapewnienie bezpieczeństwa cybernetycznego i muszą wspólnie pracować na rzecz osiągnięcia tego celu, zarówno na poziomie krajowym, jak i na poziomie UE. Ponieważ w grę mogą wchodzić różne ramy prawne i różne jurysdykcje, jednym z głównych wyzwań dla UE jest sprecyzowanie ról i obowiązków licznych zainteresowanych podmiotów.

Ze względu na złożoność zagadnienia i różnorodność zainteresowanych podmiotów, scentralizowany nadzór europejski nie jest odpowiednim rozwiązaniem. Rządy krajowe mają najlepsze warunki do organizacji działań w zakresie zapobiegania incydentom i atakom cybernetycznym i reagowania na nie oraz w zakresie nawiązywania kontaktów i współtworzenia sieci z sektorem prywatnym i z ogółem społeczeństwa, w oparciu o prowadzone już działania polityczne i istniejące ramy prawne. Jednocześnie, ze względu na potencjalny lub rzeczywisty transgraniczny charakter zagrożeń, skuteczna reakcja na poziomie krajowym często wymaga zaangażowania na poziomie UE. W celu rozwiązania

problemu bezpieczeństwa cybernetycznego w kompleksowy sposób działania powinny obejmować trzy filary – bezpieczeństwo sieci i informacji, egzekwowanie przepisów i obronę – które również funkcjonują w oparciu o różne ramy prawne:



3.1. Koordynacja między właściwymi organami ds. bezpieczeństwa sieci i informacji /CERT, organami egzekwowania prawa i organami obrony

Poziom krajowy

Państwa członkowskie powinny już posiadać, bądź powinny utworzyć w wyniku niniejszej strategii, struktury przeznaczone do działań w zakresie odporności cybernetycznej, cyberprzestępczości i obrony; powinny też osiągnąć poziom zdolności wymagany do celów reagowania na incydenty cybernetyczne. Jednak z uwagi na fakt, że kilka podmiotów może mieć obowiązki operacyjne dotyczące różnych aspektów bezpieczeństwa cybernetycznego, a także biorąc pod uwagę znaczenie udziału sektora prywatnego, na poziomie krajowym należy zapewnić optymalną koordynację z udziałem różnych ministerstw. Państwa członkowskie powinny określić w swoich krajowych strategiach bezpieczeństwa cybernetycznego role i obowiązki poszczególnych podmiotów krajowych.

Należy wspierać wymianę informacji między podmiotami krajowymi oraz między nimi a sektorem prywatnym, tak aby umożliwić państwom członkowskim i sektorowi prywatnemu posiadanie ogólnego obrazu różnych zagrożeń oraz lepsze zrozumienie nowych tendencji i technik wykorzystywanych zarówno do przeprowadzania cyberataków, jak i do szybszego reagowania na nie. Dzięki ustanowieniu krajowych planów współpracy w zakresie bezpieczeństwa sieci i informacji, które miałyby być wykorzystywane w przypadku incydentów cybernetycznych, państwa członkowskie powinny być w stanie dokonać wyraźnego podziału ról i obowiązków oraz zapewnić optymalność podejmowanych działań.

Poziom unijny

Podobnie jak na poziomie krajowym, na poziomie UE istnieje szereg podmiotów zajmujących się kwestiami bezpieczeństwa cybernetycznego. W szczególności trzy agencje – ENISA, Europol/EC3 i EAO – prowadzą działania w obszarach, odpowiednio, bezpieczeństwa sieci i informacji, egzekwowania prawa i obrony. Agencje te posiadają rady zarządzające, w których reprezentowane są państwa członkowskie i które stanowią platformy koordynacji na poziomie UE.

ENISA, Europol/EC3 i EAO będą zachęcane do koordynacji i współpracy w dziedzinach, w których wspólnie prowadzą działania, zwłaszcza w zakresie analiz tendencji, oceny zagrożeń, szkoleń i wymiany najlepszych praktyk. Powinny one ze sobą współpracować, zachowując jednocześnie swoją odrębność. Agencje te wraz z CERT-UE, Komisją i państwami członkowskimi powinny wspierać rozwój obdarzonej zaufaniem grupy ekspertów technicznych i ekspertów ds. polityki w tej dziedzinie.

Nieformalne kanały koordynacji i współpracy zostaną uzupełnione przez bardziej ustrukturyzowane powiązania. Do celów koordynacji w dziedzinie obronności można wykorzystać personel wojskowy UE oraz działający w ramach EAO zespół projektowy ds. obrony cybernetycznej. W pracach Rady Programowej Europolu/EC3 uczestniczyć będą między innymi Eurojust, CEPOL, państwa członkowskie[31], ENISA i Komisja, które będą mieć możliwość dzielenia się wiedzą ekspercką i które zagwarantują, że działania EC3 będą prowadzone w ramach współpracy partnerskiej, przy uznaniu znaczenia dodatkowej wiedzy specjalistycznej oraz z poszanowaniem mandatów wszystkich zainteresowanych stron. Nowy mandat ENISA powinien umożliwić wzmocnienie jej powiązań z Europolem i z zainteresowanymi stronami z branży. Najważniejszy jest jednak fakt, że wniosek ustawodawczy Komisji w sprawie bezpieczeństwa sieci i informacji ustanawia ramy współpracy w oparciu o sieć właściwych organów krajowych ds. bezpieczeństwa sieci i informacji i uwzględnia kwestie wymiany informacji między organami ds. bezpieczeństwa sieci i informacji i organami ścigania.

Poziom międzynarodowy

Komisja oraz Wysoki Przedstawiciel zapewniają wraz z państwami członkowskimi koordynację międzynarodowych działań w dziedzinie bezpieczeństwa cybernetycznego. Komisja oraz Wysoki Przedstawiciel będą przy tym przestrzegać podstawowych wartości UE oraz będą promować pokojowe, otwarte i przejrzyste wykorzystanie technologii cybernetycznych. Komisja, Wysoki Przedstawiciel i państwa członkowskie prowadzą rozmowy na temat kierunków polityki z międzynarodowymi partnerami i organizacjami międzynarodowymi, takimi jak Rada Europy, OECD, OBWE, NATO i ONZ.

3.2. Wsparcie UE w przypadku poważnego incydentu lub ataku cybernetycznego

Poważne incydenty lub ataki cybernetyczne mogą mieć wpływ na rządy, przedsiębiorstwa i osoby fizyczne w UE. W wyniku niniejszej strategii, a w szczególności w wyniku zaproponowanej dyrektywy w sprawie bezpieczeństwa sieci i informacji, procedury zapobiegania incydentom cybernetycznym, wykrywania ich i reagowania na nie powinny ulec poprawie, a państwa członkowskie i Komisja powinny sobie wzajemnie przekazywać bardziej szczegółowe informacje na temat poważnych incydentów lub ataków cybernetycznych. Mechanizmy reagowania będą się jednak różnić w zależności od rodzaju, skali i transgranicznych następstw incydentu.

Jeżeli incydent ma poważny wpływ na ciągłość działania, w dyrektywie w sprawie bezpieczeństwa sieci i informacji proponuje się wykorzystanie krajowych lub unijnych planów współpracy w zakresie bezpieczeństwa sieci i informacji, w zależności od tego, czy incydent ma transgraniczny charakter. W tym kontekście można wykorzystać sieć właściwych organów ds. bezpieczeństwa sieci i informacji w celu wymiany informacji i zapewnienia

[31] Za pośrednictwem przedstawicieli w grupie zadaniowej UE ds. cyberprzestępczości , która składa się z szefów jednostek ds. cyberprzestępczości z państw członkowskich UE.

sobie wzajemnego wsparcia. Pozwoliłoby to na zachowanie i/lub przywrócenie dotkniętych sieci i usług.

Jeżeli incydent wydaje się mieć charakter przestępczy, należy poinformować Europol/EC3, aby wraz z organami ścigania krajów dotkniętych incydentem mógł on wszcząć dochodzenie, zachować dowody, zidentyfikować sprawców oraz sprawić, że będą oni ścigani.

Jeżeli incydent nosi znamiona szpiegostwa cybernetycznego lub ataku inicjowanego przez państwo, lub ma wpływ na bezpieczeństwo kraju, krajowe organy bezpieczeństwa i obrony ostrzegają swoich odpowiedników, tak aby wiedzieli oni, że są celem ataku, i aby mogli się odpowiednio bronić. Uruchomione zostaną mechanizmy wczesnego ostrzegania oraz, w razie konieczności, procedura zarządzania kryzysowego i inne procedury. Szczególnie poważny incydent lub atak w zakresie bezpieczeństwa cybernetycznego może stanowić wystarczającą podstawę do tego, by państwo członkowskie powołało się na klauzulę solidarności UE (art. 222 Traktatu o funkcjonowaniu Unii Europejskiej).

Jeżeli incydent wydaje się prowadzić do naruszenia danych osobowych, należy powiadomić krajowe organy ds. ochrony danych lub krajowy organ regulacyjny, zgodnie z dyrektywą 2002/58/WE.

Ponadto w przypadku wystąpienia incydentów i ataków cybernetycznych przydatne będą sieci kontaktów i wsparcie ze strony partnerów międzynarodowych. Wsparcie takie może obejmować zastosowanie środków technicznych ograniczających wpływ incydentu, prowadzenie dochodzeń oraz uruchomienie mechanizmów reagowania w sytuacjach kryzysowych.

4. WNIOSKI I DALSZE DZIAŁANIA

W niniejszej strategii bezpieczeństwa cybernetycznego Unii Europejskiej, przedstawionej przez Komisję i Wysokiego Przedstawiciela Unii do Spraw zagranicznych i Polityki Bezpieczeństwa, przedstawiono wizję UE oraz określono niezbędne działania, których celem jest uczynienie środowiska internetowego w UE najbezpieczniejszym na świecie, w oparciu o silną ochronę i wspieranie praw obywateli[32].

Wizję tę można zrealizować jedynie na zasadzie prawdziwego partnerstwa między wieloma podmiotami, które muszą wziąć na siebie odpowiedzialność za stojące przed nimi wyzwania.

Komisja oraz Wysoki Przedstawiciel zwracają się zatem do Rady i Parlamentu Europejskiego o zatwierdzenie niniejszej strategii i pomoc w realizacji określonych w niej działań. Silne poparcie i zaangażowanie konieczne jest również ze strony sektora prywatnego oraz

[32] Finansowanie strategii nastąpi ze środków przewidzianych dla poszczególnych obszarów polityki (instrument „Łącząc Europę", „Horyzont 2020", Fundusz Bezpieczeństwa Wewnętrznego, WPZiB i współpraca zewnętrzna, w szczególności Instrument na rzecz Stabilności), zgodnie z wnioskiem Komisji dotyczącym wieloletnich ram finansowych na okres 2014-2020 (z zastrzeżeniem zatwierdzenia przez władzę budżetową oraz akceptacji ostatecznych kwot w wieloletnich ramach finansowych na lata 2014-2020). Ze względu na konieczność zapewnienia całkowitej zgodności z liczbą stanowisk dla agencji zdecentralizowanych oraz podpułapem dla agencji zdecentralizowanych w każdej pozycji wydatków w następnych wieloletnich ramach finansowych, agencje (CEPOL, EAO, ENISA, Eurojust i Europol/EC3), od których zgodnie z niniejszym komunikatem oczekuje się podjęcia nowych zadań, będą do tego zachęcane, o ile ustalona zostanie zdolność danej agencji do wchłonięcia rosnących zasobów i po zidentyfikowaniu wszystkich możliwości przesunięć.

społeczeństwa obywatelskiego, będących głównymi podmiotami odpowiedzialnymi za zwiększenie poziomu bezpieczeństwa i ochronę praw obywateli.

Nadszedł czas na podjęcie działstronami, aby zapewnić Europie niezbędne bezpieczeństwo. Aby sprawdzić, czy strategia jest realizowana zgodnie z planem oraz aby ocenić ją w kontekście ewentualnych zmian sytuacji, za rok Komisja i Wysoki Przedstawiciel zaproszą wszystkie zainteresowane ań. Komisja oraz Wysoki Przedstawiciel są zdecydowani współpracować ze wszystkimi zainteresowanymi strony na konferencję wysokiego szczebla w celu dokonania oceny postępów.