Rada
Unii Europejskiej

Bruksela, 19 listopada 2018 r.
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

WYNIK PRAC

Od:	Sekretariat Generalny Rady
Data:	19 listopada 2018 r.
Do:	Delegacje
Dotyczy:	Ramy polityki UE w zakresie cyberobrony (aktualizacja 2018 r.)

W załączeniu delegacje otrzymują ramy polityki UE w zakresie cyberobrony (aktualizacja 2018 r.) przyjęte przez Radę na jej 3652. posiedzeniu w dniu 19 listopada 2018 r.

ZAŁĄCZNIK

RAMY POLITYKI UE W ZAKRESIE CYBEROBRONY

(zaktualizowane w 2018 r.)

Zakres i cele

Aby odpowiedzieć na zmieniające się wyzwania dotyczące bezpieczeństwa, UE i jej państwa członkowskie muszą wzmocnić cyberodporność i rozwinąć solidne zdolności w zakresie cyberbezpieczeństwa i cyberobrony.

Ramy polityki UE w zakresie cyberobrony wspierają rozwój zdolności państw członkowskich UE w zakresie cyberobrony, a także wzmocnienie cyberochrony unijnej infrastruktury bezpieczeństwa i infrastruktury obronnej, bez uszczerbku dla krajowych przepisów państw członkowskich i prawodawstwa unijnego, w tym – o ile jest on określony – zakresu cyberobrony.

Obok przestrzeni lądowej, morskiej, powietrznej i kosmicznej cyberprzestrzeń jest piątym obszarem działań: pomyślna realizacja misji i operacji UE jest w coraz większym stopniu uzależniona od nieprzerwanego dostępu do bezpiecznej cyberprzestrzeni, a zatem wymaga solidnych i odpornych zdolności operacyjnych w cyberprzestrzeni.

Celem zaktualizowanych ram polityki UE w zakresie cyberobrony jest dalszy rozwój polityki UE w zakresie cyberobrony poprzez uwzględnienie istotnych zmian w ramach innych istotnych forów i obszarów polityki oraz podczas wdrażania ram polityki UE w zakresie cyberobrony od 2014 r. Wskazuje się w nich obszary priorytetowe dla cyberobrony i wyjaśnia role poszczególnych podmiotów europejskich przy pełnym poszanowaniu obowiązków i kompetencji podmiotów unijnych i państw członkowskich, a także ram instytucjonalnych i autonomii decyzyjnej UE.

Kontekst

W konkluzjach Rady Europejskiej w sprawie WPBiO z grudnia 2013 r. oraz w konkluzjach Rady w sprawie WPBiO z listopada 2013 r. wezwano do opracowania ram polityki UE w zakresie cyberobrony na podstawie wniosku Wysokiego Przedstawiciela, we współpracy z Komisją Europejską i Europejską Agencją Obrony (EDA). Rada przyjęła ramy polityki UE w zakresie cyberobrony w dniu 18 listopada 204 r.[1] i od tamtej pory konkretne wyniki ich wdrażania przyczyniły się do znacznego zwiększenia zdolności państw członkowskich w zakresie cyberobrony. Jako element rocznego sprawozdania z wdrażania ram polityki UE w zakresie cyberobrony (2017)[2] oraz uwzględniając inicjatywy UE w dziedzinie bezpieczeństwa i obrony, w szczególności skoordynowany roczny przegląd w zakresie obronności (CARD), stałą współpracę strukturalną (PESCO), Europejski Fundusz Obronny (EDF) oraz umowę w zakresie cywilnego wymiaru WPBiO, a także przeprowadzony w 2018 r. przegląd planu rozwoju zdolności (CDP) i planu rozwoju zdolności cywilnych (CCDP), państwa członkowskie wystąpiły z apelem, by zaktualizować ramy polityki UE w zakresie cyberobrony.

Cyberbezpieczeństwo jest jednym z priorytetów przewidzianych w globalnej strategii na rzecz polityki zagranicznej i bezpieczeństwa UE oraz w ramach poziomu ambicji UE[3]. W globalnej strategii podkreślono potrzebę zwiększenia zdolności w zakresie ochrony UE i jej obywateli oraz reagowania na kryzysy zewnętrzne. Zaznaczono też, że UE jako wspólnota bezpieczeństwa musi zostać wzmocniona. W tym kontekście działania w zakresie bezpieczeństwa i obrony powinny również zwiększyć strategiczną rolę UE i jej zdolność do niezależnego działania, gdy jest to konieczne, oraz do współdziałania z partnerami, gdy będzie to możliwe. Cele te wymagają większej współpracy w rozwijaniu zdolności przy jednoczesnym wspieraniu skuteczności i interoperacyjności wynikających z tego zdolności cywilnych i wojskowych.

---

1 Dokument Rady 15585/14 z 18.11.2014.
2 Dokument Rady 15870/17 z 19.12.2017.
3 Konkluzje Rady w sprawie realizacji globalnej strategii UE w dziedzinie bezpieczeństwa i obrony, 14.11.2016.

Wspólny zestaw propozycji w sprawie realizacji wspólnej deklaracji podpisanej przez przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego w Warszawie w dniu 8 lipca 2016 r.[4] obejmuje konkretne działania mające na celu rozszerzenie zakresu współpracy między UE i NATO w dziedzinie cyberbezpieczeństwa i cyberobrony, w tym w ramach misji i operacji, jak również w związku z rozwijaniem zdolności w zakresie cyberobrony, badań i technologii, szkoleń, edukacji i ćwiczeń oraz uwzględnianiem kwestii cyberbezpieczeństwa w zarządzaniu kryzysowym. Współpraca ta odbywa się z pełnym poszanowaniem zasad otwartości, przejrzystości, inkluzywności, wzajemności i autonomii decyzyjnej UE. Porozumienie techniczne między unijnym zespołem reagowania na incydenty komputerowe (CERT-UE) a komórką NATO ds. reagowania na incydenty komputerowe (NCIRC), podpisane w lutym 2016 r., ułatwia wymianę informacji technicznych, aby sprawniej zapobiegać cyberincydentom, poprawić ich wykrywanie i reagowanie na nie w obu organizacjach.

Należy przypomnieć, że niektóre polityki UE przyczyniają się do realizacji celów polityki cyberobrony przedstawionych w niniejszym dokumencie; ramy te uwzględniają również odpowiednie uregulowania, politykę i wsparcie technologiczne w dziedzinie cywilnej. Na przykład w lipcu 2016 r. Parlament Europejski i Rada przyjęły dyrektywę w sprawie bezpieczeństwa sieci i informacji[5], co doprowadzi do zwiększenia ogólnej gotowości państw członkowskich do zwalczania cyberzagrożeń oraz do pogłębienia ogólnounijnej współpracy. Dyrektywa ta ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego. Termin transpozycji dyrektywy upłynął w dniu 9 maja 2018 r.

---

4 Konkluzje Rady w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego (6 grudnia 2016 r., 15283/16; 5 grudnia 2017 r., 14802/17).

5 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 (Dz.U. L 194 z 19.7.2016, s. 1).

Przedłożony we wrześniu 2017 r. unijny akt w sprawie cyberbezpieczeństwa przewiduje nowe uprawnienia unijnej agencji cyberbezpieczeństwa (ENISA) oraz ustanowienie ogólnounijnych ram certyfikacji. Po wdrożeniu ramy certyfikacji powinny wspierać wysokie standardy procesów, produktów i usług ICT oraz być źródłem przewagi konkurencyjnej i przyczyniać się do zwiększenia zaufania ze strony konsumentów i nabywców. Ponadto, we wrześniu 2017 r. Komisja podjęła kolejne działanie, by przygotować UE na wystąpienie dużych transgranicznych incydentów w dziedzinie cyberbezpieczeństwa (plan działania), a obecnie współpracuje z państwami członkowskimi oraz innymi instytucjami, agencjami i organami, by rozwijać europejską współpracę w sytuacji kryzysu w dziedzinie cyberbezpieczeństwa, poprzez operacjonalizację i dokumentację wszystkich stosownych podmiotów, procesów i procedur w kontekście istniejących unijnych mechanizmów zarządzania kryzysowego i zarządzania klęskami żywiołowymi, a w szczególności zintegrowanych uzgodnień dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych.

W konkluzjach Rady z listopada 2016 r. w sprawie wzmacniania europejskiego systemu odporności cybernetycznej nakreślono wspólny cel polegający na przyczynianiu się do strategicznej niezależności UE, zgodnie z konkluzjami Rady z listopada 2016 r. w sprawie globalnej strategii Unii Europejskiej w zakresie polityki zagranicznej i polityki bezpieczeństwa, a także w cyberprzestrzeni. Rada Europejska potwierdziła ten cel w czerwcu 2018 r. i podkreśliła również, że należy wzmocnić zdolności w zakresie zwalczania zagrożeń w dziedzinie cyberbezpieczeństwa pochodzących spoza UE.

W 2017 r. Rada przyjęła ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”)[6]. Ramy te mają zachęcać do współpracy, ułatwiać łagodzenie zagrożeń oraz długofalowo wpływać na zachowanie potencjalnych agresorów. Obejmują wykorzystanie środków wspólnej polityki zagranicznej i bezpieczeństwa, w tym także środków ograniczających, w celu zapobiegania szkodliwym działaniom w cyberprzestrzeni i reagowania na nie. Podmioty prowadzące szkodliwe działania cybernetyczne muszą zostać pociągnięte do odpowiedzialności za swoje działania; zachęca się też państwa członkowskie UE, by w sposób skoordynowany i zgodnie z zestawem narzędzi dyplomacji cyfrowej dalej rozwijały swoje zdolności do reagowania na szkodliwe działania w cyberprzestrzeni. Państwa nie powinny prowadzić ani świadomie wspierać działań w zakresie technologii informacyjnych i komunikacyjnych w sposób sprzeczny ze swoimi zobowiązaniami wynikającymi z prawa międzynarodowego ani nie powinny świadomie zezwalać na to, by ich terytorium było wykorzystywane do popełniania czynów, które są bezprawne w świetle prawa międzynarodowego, z zastosowaniem technologii informacyjnych i komunikacyjnych.

We wrześniu 2017 r. Komisja i Wysoki Przedstawiciel zaprezentowali wspólny komunikat[7] na temat cyberbezpieczeństwa określający cel, jakim jest zmniejszenie ryzyka wynikającego z nowego profilu zagrożeń. W komunikacie tym cyberobrona jest jednym z głównych obszarów działań, a ramy polityki w zakresie cyberobrony to jeden z filarów jego wdrażania w praktyce[8].

W konkluzjach Rady z listopada 2017 r. na temat kwestii cybernetycznych zauważono coraz większe powiązania między cyberbezpieczeństwem i cyberobroną oraz wezwano do pogłębienia współpracy w zakresie cyberobrony, m.in. poprzez zachęcanie do współpracy między cywilnymi i wojskowymi służbami reagowania na incydenty. Podkreślono w nich też, że szczególnie poważny cyberincydent lub cyberkryzys mogą być wystarczającą podstawą do sięgnięcia przez państwo członkowskie po unijną klauzulę solidarności lub klauzulę o wzajemnej pomocy.

---

6 Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej”), 9916/17, 7 czerwca 2017 r.

7 Wspólny komunikat do Parlamentu Europejskiego i Rady: „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE” (13 września 2017 r., JOIN(2017) 450 final).

8 Konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE” (20 listopada 2017 r., 14435/17).

W dniu 11 grudnia 2017 r. zainicjowano stałą współpracę strukturalną (PESCO). Ustanowiono ambitne, wiążące i inkluzywne ramy współpracy między 25 państwami członkowskimi; współpraca ta obejmuje zobowiązanie do zwiększenia wysiłków w ramach współpracy w zakresie cyberobrony, a także powiązanych projektów PESCO. W pierwszym zestawie projektów PESCO zidentyfikowanych w 2017 r. przez państwa członkowskie uczestniczące w PESCO znalazły się dwa projekty związane z cyberobroną: „Zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa" oraz „Platforma wymiany informacji o cyberzagrożeniach i reagowaniu na cyberincydenty". Przewiduje się kolejne zestawy projektów PESCO. W ramach PESCO będą rozwijane zdolności w zakresie cyberobrony, a dzięki temu pogłębi się współpraca między uczestniczącymi państwami członkowskimi i zwiększy interoperacyjność.

W zaktualizowanym unijnym planie rozwoju zdolności (CDP) zatwierdzonym przez Radę Sterującą EDA w czerwcu 2018 r. stwierdzono, że cyberobrona jest jednym z kluczowych elementów, i uznano konieczność podejmowania defensywnych działań cybernetycznych w każdym kontekście operacyjnym (w oparciu o zaawansowaną obecną i przewidywaną orientację sytuacyjną w cyberprzestrzeni), w tym możliwość łączenia dużych ilości danych i informacji wywiadowczych z różnych źródeł w celu wsparcia szybkiego podejmowania decyzji oraz zwiększonej automatyzacji gromadzenia danych, ich analizy i procesu podejmowania decyzji. W CDP 2018 określono priorytety dotyczące zdolności w zakresie cyberobrony w następujących obszarach: współpraca i synergie z właściwymi podmiotami w różnych obszarach cyberbezpieczeństwa i cyberobrony; działania w zakresie badań i technologii w dziedzinie cyberobrony; ramy inżynierii systemów mające zastosowanie do działań cybernetycznych; kształcenie, szkolenie, ocena i ćwiczenia (ETEE); przezwyciężenie wyzwań w zakresie cyberobrony w powietrzu, przestrzeni kosmicznej, na morzu i lądzie.

Ponadto, ostatnich kilka lat wyraźnie pokazało, że społeczność międzynarodowa musi zapobiegać konfliktom, współpracować i ustabilizować sytuację w cyberprzestrzeni. UE,– w ścisłej współpracy z innymi organizacjami międzynarodowymi, w szczególności ONZ, OBWE i Forum Regionalnym ASEAN – promuje strategiczne ramy zapobiegania konfliktom, współpracy i stabilności w cyberprzestrzeni, które obejmują: (i) stosowanie prawa międzynarodowego, a zwłaszcza całości Karty NZ, w cyberprzestrzeni; (ii) poszanowanie powszechnych niewiążących norm, przepisów i zasad odpowiedzialnego zachowania się państw; (iii) opracowywanie i wdrażanie środków budowy zaufania na szczeblu regionalnym. Ramy polityki w zakresie cyberobrony powinny również wspierać to przedsięwzięcie.

Priorytety

W zaktualizowanych ramach polityki w zakresie cyberobrony określono sześć obszarów priorytetowych. Ramy te będą się koncentrować w szczególności na rozwijaniu zdolności w zakresie cyberobrony, a także na ochronie sieci komunikacyjnych i informacyjnych związanych z WPBiO UE. Inne obszary priorytetowe obejmują: szkolenia i ćwiczenia, badania i technologię, współpracę cywilno-wojskową oraz współpracę międzynarodową. W dziedzinie szkolenia nacisk położono na zintensyfikowanie zapewnianych przez państwa członkowskie szkoleń w zakresie cyberobrony oraz szkoleń w zakresie świadomości w dziedzinie cyberbezpieczeństwa dla struktury dowodzenia w dziedzinie WPBiO. Ważne jest też, by w ramach ćwiczeń odpowiednio uwzględniać wymiar cybernetyczny, po to by poprawić zdolność UE do reagowania na kryzysy cybernetyczne i hybrydowe poprzez usprawnienie procedur podejmowania decyzji i zwiększenie dostępności informacji. Cyberprzestrzeń jest szybko rozwijającym się obszarem, a nowości technologiczne powinny być wspierane, zarówno w sferze cywilnej, jak i wojskowej. Współpraca cywilno-wojskowa w dziedzinie cybernetycznej ma kluczowe znaczenie dla zapewnienia spójnego reagowania na cyberzagrożenia. Poza tym pogłębienie współpracy z partnerami międzynarodowymi mogłoby przyczynić się do zwiększenia cyberbezpieczeństwa w UE i poza nią oraz do propagowania zasad i wartości UE.

W ramach tych przedstawiono propozycje i możliwości koordynacji między stosownymi instytucjami, organami i agencjami UE. Odzwierciedlono w nich również istotną rolę sektora prywatnego w rozwijaniu technologii w zakresie cyberbezpieczeństwa i cyberobrony.

Ponadto ramy te popierają też uwzględnianie kwestii cyberobrony w unijnych mechanizmach zarządzania kryzysowego, w przypadku których – aby przezwyciężyć skutki cyberkryzysu – mogą mieć zastosowanie stosowne postanowienia Traktatu o UE i Traktatu o funkcjonowaniu UE[9].

1. Wspieranie rozwijania zdolności państw członkowskich w zakresie cyberobrony

W ramach rozwoju zdolności i technologii w zakresie cyberobrony należy zająć się wszystkimi aspektami rozwoju zdolności, w tym doktryną, przywództwem, organizacją, personelem, szkoleniem, branżą, technologią, infrastrukturą, logistyką i interoperacyjnością. W tym celu państwa członkowskie powinny zwiększyć swoje wysiłki, by zapewnić skuteczną zdolność w zakresie cyberobrony. ESDZ, Komisja i EDA powinny współpracować i wspierać te wysiłki.

Konieczne są ciągła ocena słabych punktów infrastruktur informacyjnych, które wspierają misje i operacje w dziedzinie WPBiO, oraz przebiegające niemal w czasie rzeczywistym rozpatrywanie skuteczności ochrony. Z operacyjnego punktu widzenia działania w zakresie cyberobrony będą koncentrować się przede wszystkim na utrzymaniu dostępności, integralności i poufności sieci komunikacyjnych i informacyjnych związanych z WPBiO, chyba że mandat operacji lub misji przewiduje inaczej. Ponadto ESDZ, we współpracy z państwami członkowskimi, będzie dalej uwzględniać zdolności w zakresie cyberbezpieczeństwa w misjach i operacjach w dziedzinie WPBiO.

Podmioty prowadzące szkodliwe działania cybernetyczne muszą zostać pociągnięte do odpowiedzialności za swoje działania. Ważne jest, by państwa członkowskie UE, przy wsparciu ze strony ESDZ, wspierały wzajemną współpracę w celu reagowania na szkodliwe działania cybernetyczne. Zestaw narzędzi dla dyplomacji cyfrowej ma pomóc zapewnić takie wspólne reagowanie. W oparciu o ten zestaw narzędzi dla dyplomacji cyfrowej ESDZ i EDA będą regularnie organizować ćwiczenia, w ramach których państwa członkowskie UE będą mogły prowadzić stosowne działania w praktyce.

---

[9] Art. 222 TFUE i art. 42 ust. 7 TUE, z należytym uwzględnieniem art. 17 TUE.

Biorąc pod uwagę, że w krajowych przepisach państw członkowskich i prawodawstwie unijnym zakres cyberobrony, o ile jest on zdefiniowany, jest szeroki i zróżnicowany, istnieje potrzeba wypracowania jego wspólnego łącznego rozumienia.

Jako że podstawą operacji wojskowych w dziedzinie WPBiO jest infrastruktura dowodzenia, kontroli, łączności i informatyczna (C4) zapewniana przez państwa członkowskie, przy planowaniu wymogów w zakresie cyberobrony dotyczących infrastruktury informacyjnej niezbędny jest pewien poziom zbieżności strategicznej.

Opierając się na pracach działającego w EDA zespołu projektowego ds. cyberobrony, w celu rozwijania zdolności w zakresie cyberobrony EDA i państwa członkowskie:

- będą wykorzystywać CDP oraz inne instrumenty, takie jak CARD, które ułatwiają i wspierają współpracę między państwami członkowskimi, po to by poprawić poziom zbieżności w planowaniu wymogów państw członkowskich w zakresie cyberobrony na szczeblu strategicznym, w szczególności wymogów dotyczących monitorowania, orientacji sytuacyjnej, zapobiegania, wykrywania i ochrony, udostępniania informacji, zdolności analitycznych w zakresie forensyki i złośliwego oprogramowania, wdrożonych doświadczeń, zapobiegania rozprzestrzenianiu się szkód, zdolności w zakresie dynamicznego odtwarzania systemów, przechowywania rozesłanych danych i wykonywania kopii zapasowych;
- będą wspierać obecne i przyszłe projekty związane z cyberobroną w zakresie wspólnego pozyskiwania i wykorzystywania zdolności do celów operacji wojskowych (np. w dziedzinie forensyki, rozwoju interoperacyjności, określania norm);
- będą rozwijać – w oparciu o istniejące ogólnounijne doświadczenia – standardowy zestaw celów i wymogów określających minimalny poziom bezpieczeństwa cybernetycznego i zaufania, który mają osiągnąć państwa członkowskie.

ESDZ i EDA:

- będą ułatwiać wymianę wiedzy między państwami członkowskimi na temat krajowych doktryn w zakresie cyberobrony oraz na temat zorientowanych na cyberobronę programów dotyczących poboru, zatrzymywania i rezerwistów.

EDA:

- przeanalizuje różne zakresy wymogów wojskowych w dziedzinie cyberobrony przewidziane w krajowych przepisach i najlepszych praktykach państw członkowskich. Głównym celem analizy będzie opracowanie architektury korporacyjnej w zakresie cyberobrony, tak by obejmowała ona zakres, funkcje i wymogi stosowane w tej dziedzinie przez państwa członkowskie na podstawie przepisów krajowych i unijnych.

Państwa członkowskie na zasadzie dobrowolności:

- usprawnią współpracę między swoimi zespołami reagowania na incydenty komputerowe, tak by poprawić zapobieganie incydentom i postępowanie w przypadku ich wystąpienia;
- będą wykorzystywać PESCO do dalszego pogłębiania współpracy w dziedzinie cyberobrony, łącznie z nowymi projektami;
- będą wykorzystywać Europejski Fundusz Obronny, by wspólnie rozwijać zdolności w zakresie cyberobrony;
- wypracują wspólne rozumienie stosowania klauzuli wzajemnej pomocy w dziedzinie cyberbezpieczeństwa, przy jednoczesnym zachowaniu jej elastyczności;
- opracują podstawowe wymogi w zakresie cyberobrony dotyczące infrastruktury informacyjnej;
- w wymiarze, w jakim poprawa zdolności w zakresie cyberobrony jest uzależniona od cywilnej wiedzy fachowej na temat bezpieczeństwa sieci i informacji, będą wykorzystywać wiedzę fachową ENISA, organów państw członkowskich zebranych w grupie współpracy ds. bezpieczeństwa sieci i informacji oraz innych ewentualnych podmiotów na szczeblu UE mających wiedzę fachową w zakresie cywilnego cyberbezpieczeństwa.

Państwa członkowskie, ESDZ / Sztab Wojskowy UE, EKBiO oraz EDA:

- rozważą opracowanie szkolenia dotyczącego cyberobrony do celów certyfikacji grup bojowych UE.

Komisja we współpracy z państwami członkowskimi:

- rozważy uwzględnienie cyberobrony w programach prac Europejskiego programu rozwoju przemysłu obronnego oraz utworzenie Europejskiego Funduszu Obronnego.

2. Usprawnienie ochrony systemów komunikacyjnych i informacyjnych związanych z WPBiO wykorzystywanych przez podmioty UE

Bez uszczerbku dla roli zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT–UE) jako centralnej struktury UE koordynującej reagowanie na cyberincydenty na potrzeby wszystkich unijnych instytucji, organów i agencji oraz w ramach odpowiednich przepisów dotyczących budżetu Unii, ESDZ wypracuje odpowiednie i autonomiczne rozumienie kwestii bezpieczeństwa i obrony sieci, a także rozwinie własne zdolności w zakresie bezpieczeństwa informatycznego. Będzie dążyć do poprawy odporności sieci ESDZ związanych z WPBiO, koncentrując się na zapobieganiu, wykrywaniu, reagowaniu na incydenty, orientacji sytuacyjnej, wymianie informacji i mechanizmach wczesnego ostrzegania.

Ochroną systemów komunikacyjnych i informacyjnych ESDZ oraz rozwijaniem zdolności w zakresie bezpieczeństwa technologii informacyjnej kieruje Dyrekcja Generalna ds. Budżetu i Administracji (DG BA) w ESDZ. Dodatkowe służące temu zasoby oraz wsparcie będą zapewniane również przez Sztab Wojskowy Unii Europejskiej (EUMS), Dyrekcję ds. Zarządzania Kryzysowego i Planowania (CMPD) oraz Komórkę Planowania i Prowadzenia Operacji Cywilnych (CPCC). Te zdolności w zakresie bezpieczeństwa informatycznego będą dotyczyć zarówno systemów niejawnych, jak i jawnych, i będą integralną częścią istniejących podmiotów operacyjnych.

Konieczna jest także optymalizacja zasad bezpieczeństwa odnoszących się do systemów informacyjnych zapewnianych przez różne podmioty instytucjonalne UE podczas misji i operacji w dziedzinie WPBiO. W tym kontekście można by rozważyć ujednoliconą strukturę dowodzenia, tak aby poprawić odporność sieci wykorzystywanych do celów WPBiO.

Z myślą o lepszej koordynacji i zwiększeniu ochrony i odporności systemów i sieci komunikacyjnych i informacyjnych związanych z WPBiO, w 2017 r. w ramach ESDZ utworzono radę ds. cyberzarządzania, która podlega sekretarzowi generalnemu ESDZ.

ESDZ / DG BA:

- będą wzmacniać zdolności w zakresie bezpieczeństwa informatycznego w ramach ESDZ, w oparciu o istniejące techniczne zdolności i procedury, koncentrując się na zapobieganiu, wykrywaniu, reagowaniu na incydenty, orientacji sytuacyjnej, wymianie informacji i mechanizmie wczesnego ostrzegania. Strategia współpracy z CERT–UE i istniejącymi zdolnościami UE w zakresie cyberbezpieczeństwa będzie dalej doskonalona.

ESDZ / DG BA, wraz z EUMS, MPCC, CMPD i CPCC:

- będą rozwijać spójną politykę bezpieczeństwa informatycznego i wytyczne w tej dziedzinie – także biorąc pod uwagę wymogi techniczne cyberobrony w kontekście WPBiO na potrzeby struktur, misji i operacji oraz uwzględniając istniejące ramy i polityki współpracy w UE – tak by zapewnić zbieżność zasad, polityk i organizacji.

ESDZ / pojedyncza komórka analiz wywiadowczych (SIAC):

- w oparciu o istniejące struktury – będą wzmacniać swoje zdolności w zakresie oceny cyberzagrożeń i zdolności wywiadowcze, aby identyfikować nowe rodzaje cyberzagrożeń, i będą zapewniać regularne oceny ryzyka w oparciu o strategiczną ocenę zagrożenia i przekazywane niemal w czasie rzeczywistym informacje koordynowane między odnośnymi strukturami UE i udostępniane przy różnych klauzulach tajności.

ESDZ/SIAC oraz CERT–UE:

- będą propagować udostępnianie w czasie rzeczywistym informacji o cyberzagrożeniach pomiędzy państwami członkowskimi a odpowiednimi podmiotami UE. W tym celu w drodze podejścia opartego na dobrowolności i wykorzystującego istniejącą współpracę między odpowiednimi krajowymi i europejskimi organami opracowane zostaną mechanizmy udostępniania informacji i środki budowy zaufania.

ESDZ/EUMS oraz MPCC:

- rozwiną i włączą do planowania na szczeblu strategicznym koncepcję cyberobrony na potrzeby misji i operacji wojskowych w dziedzinie WPBiO;
- opracują, we współpracy z dowództwem operacji, ogólną standardową procedurę operacyjną w przypadku cyberzagrożenia.

ESDZ/CPCC oraz CMPD:

- rozwiną i włączą do planowania na szczeblu strategicznym koncepcję cyberobrony na potrzeby misji cywilnych w dziedzinie WPBiO;
- wzmocnią zdolności cywilne misji w dziedzinie WPBiO w zakresie cyberobrony w oparciu o istniejącą infrastrukturę oraz poprzez propagowanie ujednolicania i harmonizacji technologii stosowanych w ramach misji i operacji w dziedzinie WPBiO, w stosownych przypadkach wykorzystując wiedzę fachową CERT–UE, ENISA i EDA;
- w trakcie wzmacniania cywilnego wymiaru WPBiO dokładniej zbadają możliwości udzielania przez cywilne misje w dziedzinie WPBiO wsparcia w zakresie cyberbezpieczeństwa dla państw przyjmujących.

ESDZ:

- rozwinie wspólne wymogi dla cywilnych i wojskowych misji i operacji w dziedzinie WPBiO;
- wzmocni koordynację cyberobrony z myślą o realizacji celów związanych z ochroną sieci wykorzystywanych przez podmioty instytucjonalne UE, wspierających WPBiO, w oparciu o istniejące ogólnounijne doświadczenia;
- będzie regularnie poddawać przeglądom wymogi w zakresie zasobów oraz inne stosowne decyzje dotyczące polityki, w oparciu o zmieniające się warunki zagrożenia i w porozumieniu z państwami członkowskimi i innymi instytucjami UE.

3. Promowanie współpracy cywilno-wojskowej

Cyberprzestrzeń jest szybko rozwijającym się obszarem: nowości technologiczne powinny być wzmacniane przez systemy bezpieczeństwa, zarówno w sferze cywilnej, jak i wojskowej. W miarę możliwości należy przewidzieć koordynację między sferą cywilną a wojskową, w przypadkach gdy podobne nowości technologiczne zapewnią rozwiązania dla zastosowań cywilnych i wojskowych. W innych przypadkach zdolności wojskowe i systemy uzbrojenia są na tyle specyficzne, że nie istnieje możliwość wspólnego wykorzystania w technologiach cywilnych. Bez uszczerbku dla wewnętrznej organizacji i przepisów państw członkowskich współpraca cywilno-wojskowa w dziedzinie cyberprzestrzeni może być rozważana m.in. do celów wymiany najlepszych praktyk, mechanizmów wymiany informacji i wczesnego ostrzegania, oceny ryzyka w zakresie reagowania na incydenty i zwiększenia wiedzy na ten temat oraz szkoleń i ćwiczeń.

Poprawa cyberbezpieczeństwa w sferze cywilnej jest jednym z istotnych czynników wpływających na ogólny poziom bezpieczeństwa sieci i informacji. Dyrektywa w sprawie bezpieczeństwa sieci i informacji przyczynia się do zwiększenia gotowości na szczeblu krajowym i do zacieśnienia współpracy pomiędzy państwami członkowskimi na szczeblu Unii, zarówno na poziomie strategicznym, jak i operacyjnym. Współpraca ta obejmuje zarówno krajowe organy nadzorujące polityki dotyczące cyberbezpieczeństwa, jak i krajowe CERT i CERT–UE. Należy wzmocnić współpracę między cywilnymi i wojskowymi CERT, w należyty sposób uwzględniając te zmiany. Nowy europejski akt w sprawie cyberbezpieczeństwa ma na celu zwiększenie odporności Europy na cyberataki i zapewnienie ram certyfikacji cyberbezpieczeństwa w odniesieniu do produktów i usług, a tym samym zwiększenie zaufania w cywilnej sferze cyfrowej.

EDA, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) i CERT-UE, wraz z innymi odpowiednimi organami i agencjami UE, w ramach ich odpowiednich mandatów oraz bez nakładania się kompetencji z kompetencjami państw członkowskich, a także państwa członkowskie, są zachęcane do dalszego zacieśniania współpracy w następujących obszarach:

- opracowanie wspólnych profili kompetencji w zakresie cyberbezpieczeństwa i cyberobrony w oparciu o najlepsze praktyki międzynarodowe i międzynarodową certyfikację, stosowane przez instytucje, organy i agencje UE, w tym również z uwzględnieniem norm sektora prywatnego w zakresie certyfikacji;
- udział w dalszym rozwijaniu i dostosowywaniu norm organizacyjnych i technicznych sektora publicznego w zakresie cyberbezpieczeństwa i cyberobrony do wykorzystania przez sektor bezpieczeństwa i sektor obronny; w razie potrzeby – opieranie się na pracach prowadzonych przez ENISA i EDA;
- ustanowienie lub dalsze rozwijanie mechanizmów i ustaleń roboczych służących wymianie najlepszych praktyk, zwłaszcza w dziedzinie kształcenia, szkolenia i ćwiczeń, a także badań i technologii oraz w innych obszarach zapewniających cywilno-wojskowe synergie;
- wykorzystanie istniejących zdolności UE w zakresie zapobiegania cyberprzestępczości, prowadzenia dochodzeń oraz w dziedzinie forensyki, a także ich skuteczniejsze stosowanie do rozwijania zdolności w zakresie cyberobrony.

Państwa członkowskie na zasadzie dobrowolności:

- pogłębia współpracę między cywilnymi i wojskowymi CERT w różnych państwach członkowskich.

ESDZ, Komisja oraz państwa członkowskie:

- uwzględnią cyberobronę w unijnych procedurach zarządzania kryzysowego i zarządzania klęskami żywiołowymi (poprzez proces opracowywania planów działania).

4. Badania i technologia

Przed operatorami infrastruktury oraz dostawcami usług w zakresie technologii informacyjno-komunikacyjnej do celów cywilnych i obronnych stoją podobne wyzwania, jeśli chodzi o cyberbezpieczeństwo, co wynika ze wspólnych wymogów w zakresie zdolności technologicznych i operacyjnych. Przewiduje się, że wspólne zapotrzebowanie w zakresie badań i technologii oraz wspólne wymogi dotyczące systemów spowodują w perspektywie długoterminowej poprawę interoperacyjności systemów oraz zmniejszenie kosztów opracowywania rozwiązań. Osiągnięcie ekonomii skali jest niezbędne, aby odpowiedzieć na stale rosnącą liczbę zagrożeń i słabych punktów. Z drugiej strony powinno to ułatwić utrzymanie i wzrost konkurencyjnego przemysłu cyberobronnego w Europie.

Rozwijanie zdolności w zakresie cyberobrony ma istotny wymiar związany z badaniami i technologią. W ramach programu badań dotyczących cyberobrony (CDRA) EDA zapewniła solidną podstawę do priorytetyzacji przyszłego finansowania badań i technologii na szczeblu ram międzyrządowych. W kolejnym programie badań strategicznych opracowanym przez EDA w ramach stosownej grupy roboczej *ad hoc* przewidziano świadomą priorytetyzację technologii związanych z cyberbezpieczeństwem niezbędnych do celów wojskowych, przy czym określono możliwości prowadzenia działań i inwestycji na rzecz podwójnego zastosowania, niezależnie od tego, czy są one finansowane ze źródeł krajowych, wielonarodowych czy unijnych.

Rozwijanie zdolności technologicznych w Europie, aby ograniczyć zagrożenia i słabe punkty, jest kwestią zasadniczą. Przemysł będzie nadal główną siłą napędową związanych z cyberobroną technologii i innowacji. Kryptografia, bezpieczne systemy wbudowane, wykrywanie złośliwego oprogramowania, techniki symulacji i wizualizacji, ochrona sieci i systemów łączności, technologia identyfikowania i uwierzytelniania to niektóre z dziedzin, którymi należy się zająć. Ważne jest także, by wspierać konkurencyjny europejski przemysłowy łańcuch dostaw w dziedzinie cyberbezpieczeństwa, w tym także poprzez angażowanie małych i średnich przedsiębiorstw (MŚP).

Zdolność Europy do dotrzymania kroku międzynarodowym konkurentom, jeśli chodzi o zdolności technologiczne w zakresie cyberbezpieczeństwa, zależy także od naszej zdolności do stymulowania przełomowych innowacji przy pomocy instrumentów krajowych i unijnych, takich jak Europejska Rada ds. Innowacji.

Aby ułatwić cywilno-wojskową współpracę w rozwijaniu zdolności w zakresie cyberobrony, wzmocnić europejską bazę technologiczno-przemysłową sektora obronnego[10] i przyczynić się do strategicznej autonomii UE również w dziedzinie cyberprzestrzeni, w razie potrzeby i w miarę możliwości we współpracy z partnerami,

EDA, Komisja oraz państwa członkowskie:

- będą dążyć do synergii wysiłków w zakresie badań i technologii w sektorze wojskowym z cywilnymi programami badawczo-rozwojowymi, w szczególności programami dotyczącymi przełomowych innowacji, i będą brać pod uwagę wymiar związany z cyberbezpieczeństwem i cyberobroną przy realizacji działania przygotowawczego w zakresie badań nad obronnością;
- będą się informować o programach badań naukowych w dziedzinie cyberbezpieczeństwa (np. o programie badań strategicznych EDA w zakresie cyberbezpieczeństwa), a także o związanych z nimi harmonogramach i działaniach; w tym celu, w ścisłej współpracy z Komisją i państwami członkowskimi, opracowany zostanie program międzysektorowych badań w dziedzinie cyberobrony;
- będą przyczyniać się do lepszego uwzględniania kwestii cyberbezpieczeństwa i cyberobrony w programach, których wymiar dotyczący bezpieczeństwa i obrony związany jest z podwójnym zastosowaniem, np. w programie dotyczącym europejskiego systemu zarządzania ruchem lotniczym nowej generacji (SESAR).

[10] Komunikat „W kierunku bardziej konkurencyjnego i wydajnego sektora obronności i bezpieczeństwa”, COM (2013) 542.

Komisja:

- rozważy utworzenie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, z siecią krajowych ośrodków koordynacji, w celu wspierania zdolności technologicznych i przemysłowych w zakresie cyberbezpieczeństwa oraz zwiększenia konkurencyjności unijnego sektora cyberbezpieczeństwa, przy zapewnieniu komplementarności i unikania powielania działań w ramach sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz względem innych agencji UE. Wspomniane centrum powinno m.in. wzmocnić współdziałanie technologii i zastosowań cywilnych i obronnych, w ścisłej współpracy i przy pełnej komplementarności działań w dziedzinie cyberobrony z Europejską Agencją Obrony;
- będzie wspierać rozwijanie przemysłowych ekosystemów i klastrów innowacyjnych, obejmujących cały łańcuch wartości związany z bezpieczeństwem, poprzez korzystanie z wiedzy naukowej, innowacji MŚP i produkcji przemysłowej.

Komisja we współpracy z państwami członkowskimi:

- uwzględni kwestie cyberobrony w zaproszeniach do składania propozycji działań przygotowawczych w zakresie badań nad obronnością;
- uwzględni kwestie cyberobrony w tematach postulowanych w ramach Europejskiego Funduszu Obronnego;
- będzie wspierać spójność unijnej polityki w celu zapewnienia, by aspekty polityczne i techniczne cyberochrony UE pozostały wśród głównych celów innowacji technologicznej i były zharmonizowane w całej UE (zdolności w zakresie analizy i oceny cyberzagrożeń, inicjatywy dotyczące „uwzględniania kwestii bezpieczeństwa na etapie projektu", zarządzanie zależnościami do celów dostępu do technologii itd.).

5. Poprawa możliwości w dziedzinie kształcenia, szkolenia i ćwiczeń

Aby zwiększyć gotowość do przeciwdziałania cyberzagrożeniom i wypracować wspólną kulturę cyberobrony w całej UE, z korzyścią m.in. dla unijnych misji i operacji, należy poprawić i zwiększyć możliwości w zakresie szkoleń dotyczących cyberobrony. Bardzo ważne jest to, by budżety na kształcenie i szkolenie były wykorzystywane w sposób efektywny przy jednoczesnym zapewnieniu jak najwyższej jakości. Łączenie i udostępnianie możliwości w zakresie kształcenia i szkolenia związanego z cyberobroną na szczeblu europejskim będzie miało zasadnicze znaczenie.

Europejskie Kolegium Bezpieczeństwa i Obrony (EKBiO), ESDZ, EDA, Komisja oraz państwa członkowskie:

- ustanowią – na podstawie przeprowadzonej przez EDA analizy potrzeb szkoleniowych w zakresie cyberobrony oraz na podstawie doświadczeń zebranych w ramach szkolenia związanego z cyberbezpieczeństwem prowadzonego przez EKBiO – szkolenie i kształcenie w dziedzinie WPBiO skierowane do różnych odbiorców, w tym ESDZ, personelu misji i operacji w dziedzinie WPBiO oraz urzędników z państw członkowskich, co powinno również pomóc rozwiązać problem dotyczący zatrzymywania wykwalifikowanych pracowników w perspektywie krótko-, średnio- i długookresowej;
- zaproponują ustanowienie dialogu z państwami członkowskimi, instytucjami UE, państwami trzecimi i innymi organizacjami międzynarodowymi, a także z sektorem prywatnym, dotyczącego cyberobrony i odnoszącego się do norm i certyfikacji w zakresie szkolenia;
- będą utrzymywać kontakty z europejskimi podmiotami sektora prywatnego zapewniającymi szkolenie, a także z instytucjami akademickimi, aby zwiększyć kompetencje i umiejętności personelu biorącego udział w misjach i operacjach w dziedzinie WPBiO.

EKBiO:

- będzie dalej rozwijać ustanowioną w swoich ramach platformę kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa;
- zapewni synergie z programami szkoleń innych zainteresowanych podmiotów, takich jak ENISA, Europol, Europejskie Kolegium Policyjne (CEPOL) i natowskie Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi;
- zbada możliwość ustanowienia przez EKBiO i NATO wspólnych programów szkolenia w zakresie cyberobrony, dostępnych dla wszystkich państw członkowskich UE, aby wspierać wspólną kulturę cyberobrony.

Komisja:

- oceni sposoby zwiększenia możliwości szkolenia i kształcenia w państwach członkowskich wskazane przez platformę kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa.

EDA:

- we współpracy z EKBiO będzie opracowywać swoje kolejne kursy, tak by spełnić wymagania państw członkowskich w zakresie kształcenia, szkolenia i ćwiczeń związanych z cyberobroną;
- będzie wspierać platformę kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa, m.in. poprzez stopniowe włączanie modułów dotyczących kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa opracowanych w ramach EDA.

ESDZ i państwa członkowskie:

- będą stosować ustanowione przez EKBiO mechanizmy certyfikacji programów szkoleniowych w ścisłym porozumieniu z odpowiednimi służbami instytucji, organów i agencji UE w oparciu o istniejące normy i wiedzę; rozważą możliwość ustanowienia specjalnych modułów dotyczących kwestii cybernetycznych w ramach inicjatywy „wojskowy Erasmus”.

Konieczna jest poprawa możliwości w zakresie ćwiczeń dotyczących cyberobrony przeznaczonych dla wojskowych i cywilnych podmiotów WPBiO. Wspólne ćwiczenia są narzędziem służącym do rozwijania wspólnej wiedzy i jednakowego rozumienia cyberobrony. Pozwoli to siłom krajowym zwiększyć gotowość do działania w środowisku wielonarodowym. Prowadzenie wspólnych ćwiczeń dotyczących cyberobrony posłuży ponadto budowie interoperacyjności i zaufania.

ESDZ, EDA, CERT-UE i państwa członkowskie skoncentrują się na propagowaniu elementów związanych z cyberobroną w ramach ćwiczeń w dziedzinie WPBiO i w innych dziedzinach:

- będą uwzględniać wymiar dotyczący cyberobrony w istniejących scenariuszach ćwiczeń *MILEX* i *MULTILAYER*;
- będą regularnie organizować ćwiczenia strategiczne/polityczne, takie jak *CYBRID 2017*, koordynując je z prowadzonym przez UE równoległym i skoordynowanym ćwiczeniem (PACE), a także ćwiczenia techniczno-operacyjne, takie jak *DEFNET*;
- opracują, w stosownych przypadkach, specjalne unijne ćwiczenie poświęcone cyberobronie w dziedzinie WPBiO i zbadają możliwość koordynacji z ogólnoeuropejskimi ćwiczeniami w zakresie cyberbezpieczeństwa, takimi jak *CyberEurope*, organizowanymi przez ENISA;
- będą w dalszym ciągu uczestniczyć w innych wielonarodowych ćwiczeniach w zakresie cyberobrony, takich jak *Locked Shields*;
- do udziału w ćwiczeniach zaproszą odpowiednich partnerów międzynarodowych, np. NATO, zgodnie z unijnymi ramami polityki ćwiczeń;
- w oparciu o zestaw narzędzi dla dyplomacji cyfrowej zorganizują regularne ćwiczenia, w ramach których państwa członkowskie UE mogą przećwiczyć reagowanie na szkodliwe działania w cyberprzestrzeni.

6. Zacieśnianie współpracy z odpowiednimi partnerami międzynarodowymi

W ramach współpracy międzynarodowej konieczne jest zapewnienie dialogu z partnerami międzynarodowymi, a konkretnie z NATO i innymi organizacjami międzynarodowymi, aby przyczynić się do rozwijania skutecznych zdolności w zakresie cyberobrony. Należy dążyć do większego zaangażowania w prace prowadzone w ramach Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE) i Organizacji Narodów Zjednoczonych (ONZ) z myślą o przedstawieniu strategicznych ram zapobiegania konfliktom, współpracy i stabilności w cyberprzestrzeni.

W UE istnieje wola polityczna, by dalej współpracować z NATO w kwestii cyberobrony w celu rozwinięcia solidnych i odpornych zdolności w zakresie cyberobrony zgodnie z wymogami zawartymi we wspólnej deklaracji podpisanej przez przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego w dniu 8 lipca 2016 r. w Warszawie. Regularne konsultacje między personelem, wzajemne briefingi, a także możliwe spotkania Grupy Polityczno-Wojskowej z odpowiednimi komitetami NATO pozwolą zapobiec zbędnemu powielaniu działań oraz zapewnić spójność i wzajemne uzupełnianie się wysiłków, zgodnie ze wspomnianymi ramami współpracy.

ESDZ i EDA, wraz z państwami członkowskimi, będą dalej rozwijać współpracę między UE a NATO w dziedzinie cyberobrony, z należytym poszanowaniem ram instytucjonalnych i autonomii decyzyjnej wspomnianych organizacji:

- zintensyfikują obecne działania służące realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego;
- będą wymieniać najlepsze praktyki w zakresie zarządzania kryzysowego, a także w zakresie cyberobrony w kontekście misji i operacji wojskowych i cywilnych;
- będą pracować nad spójnością wyników przy opracowywaniu wymogów odnoszących się do zdolności w zakresie cyberobrony, w przypadku gdy nakładają się na siebie, zwłaszcza przy rozwijaniu zdolności w zakresie cyberobrony w dłuższej perspektywie;
- będą w większym stopniu wykorzystywać ramy współpracy EDA z natowskim Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi działającym jako pierwsza platforma zacieśnionej współpracy w ramach wielonarodowych projektów w zakresie cyberobrony w oparciu o właściwe oceny.

EKBiO, ESDZ i EDA:

- wzmocnią współpracę dotyczącą koncepcji szkolenia i kształcenia, a także ćwiczeń w zakresie cyberobrony;
- zapewnią wzajemny udział pracowników w ćwiczeniach, zgodnie z ustalonymi ramami.

CERT-UE:

- będzie w dalszym ciągu wykorzystywać porozumienie techniczne między CERT–UE a komórką NATO ds. reagowania na incydenty komputerowe (NCIRC), aby ulepszyć orientację sytuacyjną, wymianę informacji i mechanizmy wczesnego ostrzegania oraz przewidywać zagrożenia, które mogą mieć wpływ na obie organizacje.

Jeśli chodzi o inne organizacje międzynarodowe i odpowiednich międzynarodowych partnerów UE, ESDZ oraz państwa członkowskie, stosownie do potrzeb:

- będą śledzić rozwój wydarzeń w wymiarze strategicznym i prowadzić konsultacje w kwestiach cyberobrony z partnerami międzynarodowymi (organizacjami międzynarodowymi i państwami trzecimi);
- zbadają możliwości współpracy w kwestiach cyberobrony, w tym z państwami trzecimi uczestniczącymi w misjach i operacjach w dziedzinie WPBiO;
- w ramach stosownych organizacji międzynarodowych, w szczególności ONZ, OBWE i Forum Regionalnym ASEAN, będą wspierać stosowanie istniejącego prawa międzynarodowego, zwłaszcza całości Karty NZ, w cyberprzestrzeni, opracowywanie i wdrażanie powszechnych, niewiążących norm odpowiedzialnego zachowania się państw oraz środków budowy zaufania między poszczególnymi państwami na szczeblu regionalnym, aby zwiększyć przejrzystość i zmniejszyć ryzyko powstania nieprawdziwych wyobrażeń o działaniach podejmowanych przez państwa.

Komisja i ESDZ:

- w stosownych przypadkach będą wspierać budowanie przez partnerów UE zdolności w dziedzinie cyberbezpieczeństwa za pośrednictwem zmienionego Instrumentu na rzecz Przyczyniania się do Stabilności i Pokoju.

Działania następcze

W ramach koordynacji przez ESDZ wdrażania ram polityki w zakresie cyberobrony, aby ocenić wdrażanie tych ram polityki, ESDZ/EDA/Komisja powinny przedstawić Grupie Polityczno-Wojskowej, przy udziale członków Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni, oraz Komitetowi Politycznemu i Bezpieczeństwa roczne sprawozdanie z postępu prac obejmujące sześć wymienionych wyżej obszarów. Zaprezentowane zostanie również półroczne sprawozdanie ustne.

Kwestią zasadniczą jest, by w miarę jak ewoluują cyberzagrożenia, wskazywać nowe wymogi w zakresie cyberobrony, a następnie włączać je do ram polityki w tej dziedzinie. Następny przegląd ram polityki w zakresie cyberobrony należy przedstawić nie później niż w połowie 2022 r., w ścisłej współpracy z państwami członkowskimi.