Rada
Unii Europejskiej

Bruksela, 18 listopada 2014 r.
(OR. en)

15585/14

COPS 303
POLMIL 103
CYBER 61
RELEX 934
JAI 880
TELECOM 210
CSC 249
CIS 13
COSI 114

WYNIK PRAC

Od:	Rada
Data:	17 i 18 listopada 2014 r.
Nr poprz. dok.:	15193/14 + COR 1 COPS 287 POLMIL 97 CYBER 58 RELEX 897 JAI 845 TELECOM 196 CSC 242 CIS 12 COSI 111
Dotyczy:	Ramy polityki UE w zakresie cyberobrony

Delegacje znajdą przedstawione w załączniku ramy polityki UE w zakresie cyberobrony.

zatwierdzone przez Radę 18 listopada 2014 r.

RAMY POLITYKI UE W ZAKRESIE CYBEROBRONY

Kontekst i cele

O cyberprzestrzeni mówi się często jako o piątym obszarze działalności wojskowej, który jest równie istotny dla wspólnej polityki bezpieczeństwa i obrony (WPBiO) Unii Europejskiej (UE) jak przestrzeń lądowa, morska, powietrzna i kosmiczna. Skuteczne wdrażanie WPBiO coraz bardziej zależy od dostępności chronionej cyberprzestrzeni oraz od dostępu do niej. Solidne i odporne zdolności w zakresie cyberobrony są obecnie niezbędne do wsparcia struktur WPBiO oraz misji i operacji w dziedzinie WPBiO.

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).

Celem niniejszego dokumentu jest zapewnienie ram konkluzjom Rady Europejskiej i konkluzjom Rady, a także tym aspektom strategii w zakresie bezpieczeństwa cybernetycznego UE[1], które są związane z cyberobroną. Wskazuje się w nim obszary priorytetowe dla cyberobrony w dziedzinie WPBiO i wyjaśnia role poszczególnych podmiotów europejskich przy pełnym poszanowaniu odnośnych obowiązków i kompetencji podmiotów unijnych i państw członkowskich, a także ram instytucjonalnych i autonomii decyzyjnej UE. Grupa Przyjaciół Prezydencji (sprawy cyberprzestrzeni) uzgodniła proces wdrażania strategii bezpieczeństwa cybernetycznego UE.

[1] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń” z dnia 7 lutego 2013 r. i związane z nim konkluzje Rady do Spraw Ogólnych z dnia 25 czerwca 2013 r.

Przedmiotowe ramy polityki będą koncentrować się przede wszystkim na rozwijaniu zdolności w zakresie cyberobrony udostępnianych przez państwa członkowskie do celów WPBiO, a także na ochronie sieci komunikacyjnych i informacyjnych Europejskiej Służby Działań Zewnętrznych (ESDZ) mających znaczenie dla WPBiO. W dziedzinie szkolenia nacisk jest kładziony na opracowanie programów skierowanych do różnych odbiorców w ramach struktury dowodzenia w dziedzinie WPBiO. Ważne jest, by w ramach ćwiczeń odpowiednio uwzględniać wymiar cybernetyczny, po to by poprawić zdolność UE do reagowania na kryzysy cybernetyczne w kontekście WPBiO, usprawnić procedury podejmowania decyzji strategicznych i umocnić konstrukcję infrastruktury informatycznej. Cyberprzestrzeń jest szybko rozwijającym się obszarem, w którym zasadniczą rolę odgrywają zdolności w zakresie podwójnego zastosowania; niezbędne jest zatem rozwijanie współpracy cywilno-wojskowej i synergii z szerzej pojętymi politykami cybernetycznymi UE, aby odpowiedzieć na nowe wyzwania wiążące się z cyberprzestrzenią przy jednoczesnym poszanowaniu wewnętrznej organizacji i kompetencji państw członkowskich.

Niniejszy dokument nakreśla zasady, które mają ułatwić współpracę z sektorem prywatnym dotyczącą rozwijania zdolności w zakresie cyberobrony, ze szczególnym naciskiem na wzmocnienie badań i technologii oraz europejskiej bazy technologiczno-przemysłowej sektora obronnego (EDTIB). Zapewnia także spójność wysiłków w zakresie cyberobrony podejmowanych przez UE i Organizację Traktatu Północnoatlantyckiego (NATO) oraz proponuje obszary współpracy między tymi podmiotami.

Ponadto cele cyberobrony powinny zostać lepiej uwzględnione w unijnych mechanizmach zarządzania kryzysowego. W stosowanych przypadkach do radzenia sobie ze skutkami kryzysów cybernetycznych mogą mieć zastosowanie odpowiednie postanowienia Traktatu UE[2] i Traktatu o funkcjonowaniu UE.

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

Priorytety ram polityki UE w zakresie cyberobrony

1. Wspieranie rozwijania związanych z WPBiO zdolności państw członkowskich w zakresie cyberobrony

Aby zapewnić odporność sieci wspierających realizację WPBiO, niezbędne jest skupienie się zarówno na poprawie ochrony zarządzanych przez ESDZ sieci łączności wykorzystywanych przez struktury WPBiO, jak i na rozwijaniu przez państwa członkowskie zdolności w zakresie cyberobrony dostępnych do celów misji i operacji w dziedzinie WPBiO. W tym względzie państwa członkowskie, ESDZ i EDA powinny współpracować, by zapewnić skuteczną zdolność 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, technologią, infrastrukturą, logistyką i interoperacyjnością.

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 funkcjonalności sieci komunikacyjnych i informacyjnych WPBiO, chyba że mandat operacji lub misji przewiduje inaczej.

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 ESDZ/EDA i państwa członkowskie:

- będą wykorzystywać plan rozwoju zdolności oraz inne instrumenty, 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;
- będą ułatwiać wymianę wiedzy między państwami członkowskimi na temat krajowych doktryn, programów szkoleń i ćwiczeń w zakresie cyberobrony, a także na temat zorientowanych na cyberobronę programów dotyczących poboru, zatrzymywania i rezerwistów;
- usprawnią dobrowolną współpracę między wojskowymi zespołami reagowania na incydenty komputerowe (CERT) państw członkowskich, aby poprawić zapobieganie incydentom i postępowanie w przypadku ich wystąpienia;
- rozważą opracowanie szkolenia dotyczącego cyberobrony do celów certyfikacji grup bojowych UE;
- w wymiarze, w jakim poprawa zdolności w zakresie cyberobrony zależy od cywilnej wiedzy fachowej na temat bezpieczeństwa sieci i informacji, państwa członkowskie mogą zwracać się o pomoc do ENISA.

2. Usprawnienie ochrony sieci łączności związanych z WPBiO wykorzystywanych przez podmioty UE

Bez uszczerbku dla roli CERT–UE jako centralnej struktury UE koordynującej reagowanie na incydenty cybernetyczne 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 mechanizmach zapobiegania, wykrywania, reagowania na incydenty, orientacji sytuacyjnej, wymiany informacji i wczesnego ostrzegania.

Ochroną systemów komunikacyjnych i informacyjnych ESDZ oraz rozwijaniem zdolności w zakresie bezpieczeństwa technologii informacyjnej kieruje Dyrekcja Zarządzająca – Zasoby (MDR) 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.

Aby poprawić ochronę sieci łączności WPBiO, MDR, EUMS, CMPD i CPCC we współpracy z Centrum Analiz Wywiadowczych UE (INTCEN):

- będą wzmacniać zdolności w zakresie bezpieczeństwa informatycznego w ramach ESDZ, w oparciu o istniejące techniczne zdolności i procedury, koncentrując się na mechanizmach zapobiegania, wykrywania, reagowania na incydenty, orientacji sytuacyjnej, wymiany informacji i wczesnego ostrzegania. Należy opracować lub – jeśli jest dostępna – dalej rozwijać strategię współpracy z CERT–UE i istniejącymi zdolnościami UE w zakresie bezpieczeństwa cybernetycznego;
- 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;
- w oparciu o istniejące struktury – będą wzmacniać zdolności w zakresie oceny zagrożenia cybernetycznego i zdolności wywiadowcze, aby identyfikować nowe rodzaje ryzyka cybernetycznego, 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;
- będą propagować udostępnianie w czasie rzeczywistym informacji o zagrożeniu cybernetycznym 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;
- opracują i włączą do planowania na szczeblu strategicznym jednolitą koncepcję cyberobrony na potrzeby operacji wojskowych[3] i misji cywilnych w dziedzinie WPBiO;
- będą wzmacniać koordynację cyberobrony z myślą o realizacji celów związanych z ochroną sieci wykorzystywanych przez podmioty instytucjonalne UE, wspierających WPBiO, w oparciu o istniejące ogólnounijne doświadczenia;
- będą regularnie poddawać przeglądom wymogi w zakresie zasobów oraz inne stosowne decyzje dotyczące polityki, w oparciu o zmieniające się warunki zagrożenia i w porozumieniu z odnośnymi grupami roboczymi Rady i innymi instytucjami UE.

[3] W przypadku operacji wojskowych obecną unijną koncepcję cyberobrony na potrzeby operacji wojskowych dowodzonych przez UE należy zaktualizować w świetle niniejszych ram polityki.

3. Propagowanie współpracy i synergii cywilno-wojskowych z szerzej pojętymi politykami cybernetycznymi UE, odpowiednimi instytucjami i agencjami UE, a także z sektorem prywatnym

Cyberprzestrzeń jest szybko rozwijającym się obszarem, w którym zasadniczą rolę odgrywają zdolności w zakresie podwójnego zastosowania, a niniejsze ramy posłużą poprawie synergii między WPBiO a innymi politykami horyzontalnymi UE (takimi jak polityka przestrzeni kosmicznej czy polityka bezpieczeństwa morskiego) i strategiami UE, takimi jak strategia bezpieczeństwa morskiego i jej plan działania. Bez uszczerbku dla wewnętrznej organizacji i ustawodawstwa państw członkowskich współpraca cywilno-wojskowa w dziedzinie cybernetycznej będzie wykorzystywać rozwijanie zdolności cybernetycznych w zakresie podwójnego zastosowania, badania i technologię, wymianę wzorcowych rozwiązań, mechanizmy wymiany informacji i wczesnego ostrzegania, oceny ryzyka w zakresie reagowania na incydenty i zwiększenie wiedzy na ten temat. Wspólne działania w dziedzinie szkoleń i ćwiczeń usprawnią współpracę i zmniejszą koszty w różnych obszarach polityki.

EDA, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[4], Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) oraz inne odpowiednie agencje UE, a także państwa członkowskie, zachęcane są – w kontekście WPBiO – do zacieśniania współpracy w następujących obszarach:

- opracowanie wspólnych profili bezpieczeństwa cybernetycznego i kompetencji w zakresie obronności w oparciu o wzorcowe rozwiązania międzynarodowe i międzynarodową certyfikację, stosowane przez instytucje 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 bezpieczeństwa cybernetycznego i cyberobrony do wykorzystania przez sektor bezpieczeństwa i sektor obronny. W razie potrzeby – opieranie się na pracach prowadzonych przez ENISA i EDA;
- opracowanie mechanizmów roboczych służących do wymiany wzorcowych rozwiązań dotyczących ćwiczeń, szkoleń i innych obszarów ewentualnej synergii cywilno-wojskowej;
- 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.

[4] W ramach mandatu ENISA i w powiązaniu z wieloletnim planem prac ENISA, bez nakładania się kompetencji z kompetencjami państw członkowskich.

Poprawa cywilnego bezpieczeństwa cybernetycznego jest jednym z istotnych czynników wpływających na ogólny poziom bezpieczeństwa sieci i informacji. Oczekuje się, że wniosek dotyczący dyrektywy w sprawie bezpieczeństwa sieci i informacji przyczyni się do zwiększenia gotowości na szczeblu krajowym i zacieśnienia współpracy pomiędzy państwami członkowskimi na szczeblu Unii, zarówno na poziomie strategicznym, jak i operacyjnym. Współpraca ta powinna obejmować krajowe organy nadzorujące polityki dotyczące bezpieczeństwa cybernetycznego oraz krajowe CERT i CERT–UE. Celem publiczno-prywatnej platformy bezpieczeństwa sieci i informacji jest określenie wzorcowych rozwiązań neutralnych technologicznie z myślą o poprawie bezpieczeństwa cybernetycznego oraz opracowanie zachęt do przyjmowania bezpiecznych rozwiązań informacyjno-komunikacyjnych.

Badania i technologia we współpracy z sektorem prywatnym i środowiskiem naukowym

Przed operatorami infrastruktury oraz dostawcami usług w zakresie technologii informacyjno-komunikacyjnej do celów cywilnych i obronnych stoją podobne wyzwania, jeśli chodzi o bezpieczeństwo cybernetyczne, 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 w perspektywie długoterminowej spowodują 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 przyszłych wydatków na badania i technologie oraz do rozwijania zdolności zarówno w środowisku krajowym, jak i europejskim.

Rozwijanie solidnych 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. Kluczowe będzie zatem utrzymanie ścisłej współpracy z sektorem prywatnym przy dążeniu w miarę możliwości do synergii z cywilnymi rozwiązaniami, usługami i zdolnościami (w szczególności w dziedzinach: kryptografii, systemów wbudowanych, wykrywania złośliwego oprogramowania, technik symulacji i wizualizacji, ochrony sieci i systemów komunikacyjnych, technologii identyfikowania i uwierzytelniania). Ważne jest także, by propagować chroniony i konkurencyjny europejski przemysłowy łańcuch dostaw w dziedzinie bezpieczeństwa cybernetycznego, w tym także poprzez angażowanie małych i średnich przedsiębiorstw.

Aby ułatwić współpracę cywilno-wojskową w rozwijaniu zdolności w zakresie cyberobrony oraz umocnić europejską bazę technologiczno-przemysłową sektora obronnego[5] zgodnie z podejściem UE dotyczącym sektora cybernetycznego, EDA wraz ze służbami Komisji, a także państwa członkowskie:

- będą dążyć do synergii wysiłków w zakresie badań i technologii w sektorze wojskowym z cywilnymi programami badawczo-rozwojowymi, takimi jak „Horyzont 2020", i będą brać pod uwagę wymiar związany z bezpieczeństwem cybernetycznym i cyberobroną przy ustanawianiu działania przygotowawczego dotyczącego badań związanych z WPBiO;
- będą się dzielić programami badań naukowych w dziedzinie bezpieczeństwa cybernetycznego wśród instytucji i agencji UE (np. program badań naukowych w dziedzinie cyberobrony), w szczególności poprzez europejskie ramy współpracy, oraz dzielić się związanymi z nimi harmonogramami i działaniami;
- będą wspierać rozwijanie przemysłowych ekosystemów i klastrów innowacyjnych, obejmujących cały łańcuch wartości związany z bezpieczeństwem, poprzez korzystanie z wiedzy naukowej, innowacji MŚP i produkcji przemysłowej;
- będą wspierać spójność unijnej polityki w celu zapewnienia, by aspekty polityczne i techniczne ochrony cybernetycznej UE pozostały wśród głównych celów innowacji technologicznej i były zharmonizowane w całej UE (zdolności w zakresie analizy i oceny zagrożenia cybernetycznego, inicjatywy dotyczące „uwzględniania kwestii bezpieczeństwa na etapie projektu", zarządzanie zależnościami do celów dostępu do technologii itd.);
- będą przyczyniać się do lepszego uwzględniania kwestii bezpieczeństwa cybernetycznego i cyberobrony w programach, których wymiar dotyczący bezpieczeństwa i obrony związany jest z podwójnym zastosowaniem, np. w europejskim systemie zarządzania ruchem lotniczym nowej generacji (SESAR);
- będą aktywnie wspierać synergie z działaniami na rzecz opracowania polityki przemysłowej w zakresie cywilnego bezpieczeństwa cybernetycznego prowadzonymi na szczeblu krajowym przez państwa członkowskie i na szczeblu europejskim przez Komisję.

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

4. Poprawa możliwości w zakresie szkolenia, kształcenia i ćwiczeń

Szkolenie i kształcenie

Aby wypracować wspólną kulturę cyberobrony na wszystkich szczeblach struktury dowodzenia w dziedzinie WPBiO, w tym w ramach misji i operacji, konieczna jest poprawa możliwości w zakresie szkolenia związanego z cyberobroną. Ponadto w dobie kurczących się wydatków na obronę kwestią kluczową jest, 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.

ESDZ określi następujące priorytety szkoleniowe w dziedzinie WPBiO wraz z EDA, Europejskim Kolegium Bezpieczeństwa i Obrony (ESDC) i państwami członkowskimi:

- ustanowi – na podstawie przeprowadzonej przez EDA analizy potrzeb szkoleniowych w zakresie cyberobrony oraz na podstawie doświadczeń zebranych w ramach szkolenia związanego z bezpieczeństwem cybernetycznym prowadzonego przez ESDC – 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;
- zaproponuje 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;
- na podstawie przeprowadzonej przez EDA oceny wykonalności – zbada możliwość i zasadność utworzenia instrumentu szkoleniowego w dziedzinie cyberobrony na potrzeby WPBiO;
- będzie dalej rozwijać kursy EDA, tak aby spełnić wymogi dotyczące szkolenia związanego z cyberobroną w dziedzinie WPBiO;
- będzie stosować ustanowione przez ESDC mechanizmy certyfikacji programów szkoleniowych w ścisłym porozumieniu z odpowiednimi służbami instytucji UE w oparciu o istniejące normy i wiedzę. Rozważy możliwość ustanowienia specjalnych modułów dotyczących kwestii cybernetycznych w ramach inicjatywy „wojskowy Erasmus”;
- zapewni synergie z programami szkoleń innych zainteresowanych stron, takich jak ENISA, Europol, Europejska Grupa Szkolenia i Edukacji w zakresie Cyberprzestępczości (ECTEG) oraz Europejskie Kolegium Policyjne (CEPOL);
- zbada możliwość ustanowienia przez ESDC i Kolegium Obrony NATO wspólnych programów szkolenia w zakresie cyberobrony, dostępnych dla wszystkich państw członkowskich UE, aby wspierać wspólną kulturę cyberobrony;
- będzie utrzymywać kontakty z europejskimi podmiotami sektora prywatnego zapewniającymi szkolenie, a także z instytucjami akademickimi, aby zwiększyć kompetencje i umiejętności personelu biorącego udział w operacjach i misjach w dziedzinie WPBiO.

Ćwiczenia

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 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;
- opracują, w stosownych przypadkach, specjalne unijne ćwiczenie poświęcone cyberobronie w dziedzinie WPBiO i zbadają możliwość koordynacji z ogólnoeuropejskimi ćwiczeniami cybernetycznymi, takimi jak *CyberEurope*, organizowanymi przez ENISA;
- rozważą możliwość udziału w innych wielonarodowych ćwiczeniach dotyczących cyberobrony;
- po opracowaniu przez UE ćwiczenia poświęconego cyberobronie w dziedzinie WPBiO – będą angażować odpowiednich partnerów międzynarodowych, takich jak OBWE i NATO, zgodnie z unijną polityką ćwiczeń.

5. 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).

W UE istnieje polityczna wola prowadzenia dalszej współpracy z NATO w kwestii cyberobrony na rzecz rozwijania solidnych i odpornych zdolności w zakresie cyberobrony zgodnie z wymogami niniejszych ram polityki. Regularne konsultacje między personelem, wzajemne briefingi, a także możliwe spotkania Grupy Polityczno-Wojskowej z odpowiednimi komitetami NATO pozwalają zapobiec zbędnemu powielaniu działań oraz zapewnić spójność i wzajemne uzupełnianie się wysiłków, zgodnie z istniejącymi ramami współpracy z NATO.

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 UE:

- będą wymieniać wzorcowe rozwiązania w zakresie zarządzania kryzysowego, a także w zakresie operacji wojskowych i misji cywilnych;
- będą pracować nad spójnością opracowywania 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;
- wzmocnią współpracę dotyczącą koncepcji szkolenia i kształcenia, a także ćwiczeń w zakresie cyberobrony;
- będą bardziej wykorzystywać porozumienie o współpracy między EDA a Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi działającym w NATO jako pierwszą platformę zacieśnionej współpracy w ramach wielonarodowych projektów w zakresie cyberobrony w oparciu o właściwe oceny;
- będą zacieśniać współpracę między CERT–UE a odpowiednimi organami UE zajmującymi się cyberobroną a NCIRC (komórką NATO ds. reagowania na incydenty komputerowe), aby poprawić orientację sytuacyjną, udostępnianie informacji i mechanizmy wczesnego ostrzegania oraz przewidywać zagrożenia, które mogą mieć wpływ na oba podmioty.

Jeśli chodzi o inne organizacje międzynarodowe i odpowiednich międzynarodowych partnerów UE, ESDZ i EFA wraz z państwami członkowskimi, 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;
- będą nadal wspierać rozwijanie środków budowy zaufania w zakresie bezpieczeństwa cybernetycznego, aby zwiększyć przejrzystość i zmniejszyć ryzyko powstania nieprawdziwych wyobrażeń o działaniach podejmowanych przez państwa – przez propagowanie trwającego obecnie ustanawiania międzynarodowych norm w tej dziedzinie.

Działania następcze

Grupie Polityczno-Wojskowej oraz Komitetowi Politycznemu i Bezpieczeństwa, a także innym odpowiednim grupom roboczym Rady należy przedstawić półroczne sprawozdanie z postępów obejmujące pięć obszarów wymienionych powyżej, aby ocenić wdrażanie ram polityki. Kwestią zasadniczą jest, by w miarę jak ewoluuje zagrożenie cybernetyczne, wskazywać nowe wymogi w zakresie cyberobrony, a następnie włączać je do ram polityki w tej dziedzinie.