Consiliul
Uniunii Europene

Bruxelles, 19 noiembrie 2018
(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

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	19 noiembrie 2018
Destinatar:	Delegațiile
Subiect:	Cadrul de politici al UE pentru apărarea cibernetică (actualizare 2018)

În anexă, se pune la dispoziția delegațiilor cadrul de politici al UE pentru apărarea cibernetică (actualizare 2018), adoptat de Consiliu la cea de a 3652-a reuniune a sa, desfășurată la 19 noiembrie 2018.

ANEXĂ

CADRUL DE POLITICI AL UE PENTRU APĂRAREA CIBERNETICĂ

(astfel cum a fost actualizat în 2018)

Domeniu de aplicare și obiective

Pentru a răspunde provocărilor în continuă schimbare în materie de securitate, UE și statele sale membre trebuie să consolideze reziliența cibernetică și să dezvolte capabilități solide în domeniul securității și apărării cibernetice.

Cadrul de politici al UE pentru apărarea cibernetică (CDPF) sprijină dezvoltarea capabilităților de apărare cibernetică ale statelor membre ale UE, precum și consolidarea protecției cibernetice a infrastructurii de securitate și apărare a UE, fără a aduce atingere legislației naționale a statelor membre și legislației UE, inclusiv domeniului de aplicare al apărării cibernetice, în cazul în care acesta este definit.

Spațiul cibernetic este al cincilea domeniu de operații, alături de domeniile terestru, maritim, aerian și spațial: punerea în aplicare cu succes a misiunilor și operațiilor UE depinde din ce în ce mai mult de accesul neîntrerupt la un spațiu cibernetic sigur și, prin urmare, necesită capabilități operaționale cibernetice solide și reziliente.

Obiectivul CDPF actualizat este de a dezvolta în continuare politica de apărare cibernetică a UE luând în considerare evoluțiile pertinente din alte foruri și domenii de politică relevante, precum și punerea în aplicare a CDPF începând din 2014. CDPF identifică domeniile prioritare pentru apărarea cibernetică și clarifică rolurile diferiților actori europeni, respectând totodată pe deplin responsabilitățile și competențele actorilor Uniunii și ale statelor membre, precum și cadrul instituțional al UE și autonomia sa decizională.

Context

În concluziile Consiliului European privind PSAC din decembrie 2013, precum și în concluziile Consiliului privind PSAC din noiembrie 2013 s-a solicitat dezvoltarea unui cadru de politici al UE pentru apărarea cibernetică, pe baza unei propuneri a Înaltului Reprezentant, în cooperare cu Comisia Europeană și Agenția Europeană de Apărare (AEA). Cadrul de politici al UE pentru apărarea cibernetică a fost adoptat de Consiliu la 18 noiembrie 2014[1] și, de atunci, prin punerea sa în aplicare, au existat rezultate concrete care au contribuit la consolidarea semnificativă a capabilităților de apărare cibernetică ale statelor membre. În contextul Raportului anual din 2017 privind punerea în aplicare a cadrului de politici pentru apărarea cibernetică[2] și luând în considerare inițiativele UE în domeniul securității și apărării, în special procesul anual coordonat de revizuire privind apărarea (CARD), cooperarea structurată permanentă (PESCO), Fondul european de apărare (FEA) și pactul privind PSAC civilă, precum și revizuirea din 2018 a planului de dezvoltare a capacităților (CDP) și a planului de dezvoltare a capacităților civile (CCDP), statele membre au solicitat actualizarea cadrului de politici al UE pentru apărarea cibernetică.

Securitatea cibernetică reprezintă o prioritate în cadrul Strategiei globale pentru politica externă și de securitate a UE, precum și în cadrul nivelului de ambiție al UE[3]. Strategia globală accentuează necesitatea sporirii capacităților pentru a proteja UE și pe cetățenii săi și pentru a răspunde la crizele externe. Strategia globală subliniază necesitatea de a consolida UE ca o comunitate de securitate. În acest context, eforturile din domeniul securității și apărării ar trebui să consolideze și rolul strategic al UE și capacitatea acesteia de a acționa în mod autonom atunci când și acolo unde va fi necesar, precum și împreună cu partenerii, acolo unde va fi posibil. Realizarea acestor obiective presupune aprofundarea cooperării pentru dezvoltarea capabilităților prin promovarea eficacității și interoperabilității capabilităților civile și militare care rezultă.

---

1 Documentul 15585/14 al Consiliului, 18.11.2014.
2 Documentul 15870/17 al Consiliului, 19.12.2017.
3 Concluziile Consiliului privind punerea în aplicare a Strategiei globale a UE în domeniul securității și apărării, 14.11.2016.

Setul comun de propuneri privind punerea în aplicare a Declarației comune a președintelui Consiliului European, președintelui Comisiei Europene și secretarului general al Organizației Tratatului Atlanticului de Nord, semnată la Varșovia la 8 iulie 2016[4], cuprinde măsuri concrete de extindere a cooperării dintre UE și NATO în ceea ce privește securitatea și apărarea cibernetică, inclusiv în contextul misiunilor și al operațiilor, precum și în ceea ce privește dezvoltarea capabilităților de apărare cibernetică, cercetarea și tehnologia, activitățile de formare, educația, exercițiile și integrarea aspectelor cibernetice în gestionarea crizelor. Această cooperare se desfășoară cu respectarea deplină a principiilor deschiderii, transparenței, incluziunii, reciprocității și autonomiei decizionale a UE. Acordul tehnic semnat în februarie 2016 între Centrul de răspuns la incidente de securitate cibernetică al UE (CERT-UE) și Capacitatea de răspuns la incidente informatice a NATO (NCIRC) facilitează schimbul de informații tehnice în vederea îmbunătățirii, în cadrul ambelor organizații, a prevenirii și detectării incidentelor cibernetice și a răspunsului la acestea.

Ar trebui reamintit faptul că mai multe politici ale UE contribuie la realizarea obiectivelor politicii de apărare cibernetică, astfel cum figurează în prezentul document, iar prezentul cadru ține seama și de reglementările, politica și sprijinul tehnologic relevante din domeniul civil. De exemplu, în iulie 2016, Parlamentul European și Consiliul au adoptat Directiva privind securitatea rețelelor și a informațiilor[5] (NIS), care va ridica nivelul general de pregătire al statelor membre împotriva amenințărilor cibernetice și va consolida cooperarea la nivelul întregii UE. Această directivă stabilește măsuri în vederea obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în cadrul Uniunii, astfel încât să se îmbunătățească funcționarea pieței interne. Termenul pentru transpunerea directivei a fost 9 mai 2018.

---

4 Concluziile Consiliului privind punerea în aplicare a declarației comune a președintelui Consiliului European, președintelui Comisiei Europene și secretarului general al Organizației Tratatului Atlanticului de Nord (6 decembrie 2016, 15283/16; 5 decembrie 2017, 14802/17).

5 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, JO L 194, 19.7.2016, p. 1.

Propunerea referitoare la o lege a UE privind securitatea cibernetică, din septembrie 2017, prevede un nou mandat pentru Agenția UE pentru Securitate Cibernetică (ENISA), precum și instituirea unui cadru de certificare la nivelul UE. Odată pus în practică, acest cadru de certificare ar trebui să favorizeze standarde ridicate pentru procesele, produsele și serviciile TIC, să genereze un avantaj competitiv și să sporească încrederea consumatorilor și a achizitorilor. Tot în septembrie 2017, Comisia a mai făcut un pas în direcția pregătirii UE pentru eventualitatea unor incidente transfrontaliere de securitate cibernetică de mare amploare (*Blue Print*), iar în prezent colaborează cu statele membre și cu alte instituții, agenții și organe pentru dezvoltarea unei cooperări europene în legătură cu crizele de securitate cibernetică, instituind operaționalizarea practică și documentarea tuturor actorilor, proceselor și procedurilor relevante în contextul mecanismelor existente ale UE de gestionare a crizelor și a dezastrelor, în special al mecanismului integrat pentru un răspuns politic la crize.

În concluziile Consiliului privind consolidarea rezilienței cibernetice a Europei din noiembrie 2016 s-a evidențiat obiectivul comun de a contribui la autonomia strategică a UE, astfel cum se precizează în concluziile Consiliului din noiembrie 2016 privind Strategia globală pentru politica externă și de securitate a Uniunii Europene, inclusiv în spațiul cibernetic. Consiliul European a reiterat acest mesaj în iunie 2018 și a subliniat, de asemenea, necesitatea consolidării capabilităților de combatere a amenințărilor în materie de securitate cibernetică din afara UE.

În 2017, Consiliul a adoptat un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („setul de instrumente pentru diplomația cibernetică”)[6]. Se preconizează că acest cadru va încuraja cooperarea, va facilita atenuarea amenințărilor și va influența comportamentul potențialilor agresori pe termen lung. Acest cadru utilizează măsurile din domeniul PESC, inclusiv măsuri restrictive, pentru a preveni și a răspunde la activitățile cibernetice răuvoitoare. Actorii care desfășoară activități cibernetice răuvoitoare trebuie să fie trași la răspundere pentru acțiunile lor, iar statele membre ale UE sunt încurajate să își dezvolte în continuare capacitatea de a răspunde la activități cibernetice răuvoitoare, în mod coordonat, în conformitate cu setul de instrumente pentru diplomația cibernetică. Statele nu ar trebui să desfășoare sau să sprijine cu bună știință activități din domeniul tehnologiei informației și comunicațiilor contrare obligațiilor care le revin în temeiul dreptului internațional și nu ar trebui să permită în cunoștință de cauză ca teritoriul lor să fie utilizat pentru săvârșirea de fapte ilicite la nivel internațional care recurg la tehnologia informației și comunicațiilor.

În septembrie 2017, Comisia și ÎR/VP au prezentat o comunicare comună[7] privind chestiuni cibernetice, având drept obiectiv diminuarea riscurilor care decurg din noua situație a amenințărilor. În această comunicare, apărarea cibernetică este considerată unul dintre domeniile principale de acțiune, iar CDPF reprezintă unul dintre pilonii punerii sale concrete în aplicare[8].

În concluziile Consiliului din noiembrie 2017 privind chestiuni cibernetice s-a recunoscut legătura tot mai strânsă dintre securitatea cibernetică și apărare și s-a solicitat intensificarea cooperării în domeniul apărării cibernetice, inclusiv prin încurajarea cooperării dintre comunitățile civile și militare de răspuns în caz de incidente. De asemenea, s-a subliniat faptul că un incident sau o criză cibernetică deosebit de gravă ar putea constitui un motiv suficient pentru ca un stat membru să invoce clauza de solidaritate a UE și/sau clauza de asistență reciprocă.

---

6 Concluziile Consiliului referitoare la un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică”), 9916/17, 7 iunie 2017.

7 Comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE” [13 septembrie 2017, JOIN(2017) 450 final].

8 Concluziile Consiliului privind comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE” (20 noiembrie 2017, 14435/17).

La 11 decembrie 2017 a fost lansată cooperarea structurată permanentă (PESCO). Acest cadru de cooperare ambițios, favorabil incluziunii și cu caracter obligatoriu a fost instituit între 25 de state membre și cuprinde un angajament de intensificare a eforturilor în cadrul cooperării din domeniul apărării cibernetice, precum și în cadrul unor proiecte PESCO conexe. Primul set de proiecte PESCO identificate de statele membre participante la PESCO în 2017 cuprinde două proiecte legate de apărarea cibernetică: „Echipele de răspuns rapid în domeniul cibernetic și asistență reciprocă în ceea ce privește securitatea cibernetică” și „Platforma pentru schimbul de informații privind răspunsul la amenințările și incidentele cibernetice”. Sunt prevăzute și alte seturi de proiecte PESCO. PESCO va dezvolta capabilități de apărare cibernetică și, prin urmare, va consolida cooperarea între statele membre participante și va spori interoperabilitatea.

În versiunea actualizată a planului UE de dezvoltare a capacităților (CDP), aprobată de Comitetul director al AEA în iunie 2018, apărarea cibernetică este considerată un element-cheie, recunoscându-se necesitatea de a desfășura operațiuni cibernetice defensive în orice context operațional, pe baza unei evaluări complexe a situației actuale și preconizate a spațiului cibernetic, incluzând capacitatea de a combina volume mari de date și informații provenind din numeroase surse pentru a sprijini luarea de decizii rapide și creșterea gradului de automatizare a colectării și analizei datelor și a procesului de asistență pentru luarea deciziilor. În CDP 2018 sunt identificate prioritățile în materie de capabilități de apărare cibernetică în următoarele domenii: cooperarea și sinergiile cu actorii relevanți din domeniile apărării și securității cibernetice; activități de cercetare și tehnologice în materie de apărare cibernetică; cadrele privind ingineria sistemelor pentru operațiuni cibernetice; educația, formarea, exercițiile și evaluarea (EFEE); abordarea provocărilor legate de apărarea cibernetică din sectoarele aerian, spațial, maritim și terestru.

În sfârșit, pe parcursul ultimilor ani, a devenit evidentă necesitatea ca comunitatea internațională să prevină conflictele, să coopereze și să stabilizeze spațiul cibernetic. UE promovează, în strânsă cooperare cu alte organizații internaționale, în special cu ONU, OSCE și Forumul regional al ASEAN, un cadru strategic pentru prevenirea conflictelor, cooperare și stabilitate în spațiul cibernetic, care cuprinde (i) aplicarea dreptului internațional, în special a Cartei ONU în integralitatea sa, în spațiul cibernetic; (ii) respectarea normelor, regulilor și principiilor universale, fără caracter obligatoriu, vizând un comportament responsabil la nivel de stat; (iii) elaborarea și punerea în aplicare a unor măsuri regionale de consolidare a încrederii (CBM). Cadrul de politici al UE pentru apărarea cibernetică ar trebui să sprijine și acest demers.

Priorități

În CDPF actualizat au fost identificate șase domenii prioritare. Obiectivul primordial al acestui cadru de politici este dezvoltarea capabilităților de apărare cibernetică, precum și protejarea rețelelor de comunicații și informații din cadrul PSAC a UE. Printre celelalte domenii prioritare se numără: formarea și exercițiile, cercetarea și tehnologia, cooperarea civil-militară și cooperarea internațională. În domeniul formării, accentul se pune pe îmbunătățirea activităților de formare în domeniul apărării cibernetice desfășurate de statele membre, precum și a activităților de formare în vederea creșterii gradului de conștientizare cu privire la domeniul cibernetic la nivelul lanțului de comandă din cadrul PSAC. De asemenea, este important ca dimensiunea cibernetică să fie abordată în mod corespunzător în cadrul exercițiilor pentru a se îmbunătăți capacitatea UE de a reacționa la crizele cibernetice și hibride, prin îmbunătățirea procedurilor decizionale și a disponibilității informației. Spațiul cibernetic este un domeniu în rapidă evoluție, iar noile evoluții tehnologice trebuie să fie sprijinite, atât în domeniul civil, cât și în domeniul militar. Cooperarea civil-militară în domeniul cibernetic este esențială pentru a se asigura un răspuns coerent la amenințările cibernetice. Nu în ultimul rând, consolidarea cooperării cu partenerii internaționali ar putea contribui la consolidarea securității cibernetice atât în UE, cât și în afara acesteia, precum și la promovarea principiilor și valorilor UE.

Acest cadru prezintă propuneri și oportunități de coordonare între instituțiile, organele și agențiile relevante ale UE. De asemenea, acesta reflectă rolul important al sectorului privat pentru dezvoltarea de tehnologii în domeniul securității cibernetice și al apărării cibernetice.

În plus, CDPF furnizează un sprijin suplimentar pentru integrarea apărării cibernetice în mecanismele Uniunii de gestionare a crizelor, în cadrul cărora ar putea fi aplicate dispozițiile relevante din Tratatul privind UE și din Tratatul privind funcționarea UE[9], în vederea abordării efectelor unei crize cibernetice.

1. Sprijinirea dezvoltării capabilităților de apărare cibernetică ale statelor membre

Dezvoltarea capabilităților și a tehnologiilor de apărare cibernetică ar trebui să abordeze toate aspectele dezvoltării capabilităților, inclusiv doctrina, conducerea, organizarea, personalul, formarea, industria, tehnologia, infrastructura, logistica și interoperabilitatea. În acest scop, statele membre ar trebui să își intensifice eforturile de a asigura capabilități eficace de apărare cibernetică. SEAE, Comisia și AEA ar trebui să coopereze și să sprijine aceste eforturi.

Este necesară o evaluare continuă a vulnerabilităților infrastructurilor informaționale care sprijină misiunile și operațiile PSAC, dublată de determinarea aproape în timp real a eficacității protecției. Din punct de vedere operațional, unul dintre principalele domenii de interes al activităților de apărare cibernetică va fi menținerea disponibilității, integrității și confidențialității rețelelor de comunicații și informații în cadrul PSAC, cu excepția cazului în care se prevede altfel în mandatul operațiilor sau al misiunilor. În plus, SEAE, în cooperare cu statele membre, va spori integrarea capabilităților cibernetice în misiunile și operațiile PSAC.

Actorii responsabili de activități cibernetice răuvoitoare trebuie trași la răspundere pentru acțiunile lor. Este important ca statele membre ale UE, sprijinite de SEAE, să promoveze cooperarea reciprocă pentru a răspunde la activitățile cibernetice răuvoitoare. Setul de instrumente pentru diplomația cibernetică este elaborat pentru a sprijini realizarea unui astfel de răspuns comun. SEAE și AEA vor organiza exerciții periodice pe baza setului de instrumente pentru diplomația cibernetică în cadrul cărora statele membre ale UE pot exersa acest lucru.

---

9 Articolul 222 din TFUE și articolul 42 alineatul (7) din TUE, cu luarea în considerare în mod corespunzător a articolului 17 din TUE.

Având în vedere că domeniul de aplicare al apărării cibernetice în cadrul legislației naționale a statelor membre și al legislației UE este amplu și diversificat, acolo unde și atunci când acesta este definit, este necesară dezvoltarea unei înțelegeri comune globale a domeniului de aplicare al apărării cibernetice.

Întrucât operațiile militare din cadrul PSAC se bazează pe o infrastructură de comandă, control, comunicații și computere (C4) furnizată de statele membre, este necesar un anumit grad de convergență strategică în planificarea cerințelor de apărare cibernetică pentru infrastructura informațională.

Pe baza lucrărilor echipei proiectului de apărare cibernetică a AEA pentru dezvoltarea capabilităților de apărare cibernetică, AEA și statele membre:

- vor utiliza CDP și alte instrumente, precum CARD, care facilitează și sprijină cooperarea dintre statele membre pentru a spori gradul de convergență în planificarea cerințelor de apărare cibernetică ale statelor membre la nivel strategic, în special în ceea ce privește monitorizarea, conștientizarea situației, prevenirea, detectarea și protecția, schimbul de informații, criminalistica și capacitatea de analiză a programelor malware, lecțiile învățate, reducerea prejudiciilor, capacitățile de redresare dinamică, stocarea datelor distribuite și copiile de siguranță ale datelor;
- vor sprijini proiectele actuale și viitoare de grupare și utilizare în comun legate de apărarea cibernetică pentru operațiile militare (de exemplu în criminalistică, dezvoltarea interoperabilității, stabilirea de standarde);
- vor dezvolta un set standard de obiective și cerințe care să definească nivelul minim de securitate cibernetică și de încredere care trebuie atins de către statele membre, pe baza experienței existente pe teritoriul UE.

SEAE și AEA:

- vor facilita schimburile dintre statele membre cu privire la doctrinele naționale în domeniul apărării cibernetice, precum și cu privire la programele de recrutare și păstrare și a celor dedicate rezerviștilor orientate către apărarea cibernetică.

AEA:

- va studia diferitele domenii de aplicare ale cerințelor militare în materie de apărare cibernetică în legislația națională a statelor membre, precum și bunele practici. Principalul obiectiv al studiului respectiv este de a dezvolta o arhitectură de întreprindere pentru apărarea cibernetică pentru a include domeniul de aplicare, funcționalitățile și cerințele utilizate în acest domeniu de către statele membre pe baza legislației naționale și a legislației UE.

Statele membre, pe bază voluntară:

- vor îmbunătăți cooperarea dintre CERT-urile lor militare pentru a îmbunătăți prevenirea și gestionarea incidentelor;
- vor valorifica PESCO pentru a spori în continuare cooperarea în ceea ce privește apărarea cibernetică, inclusiv în cadrul unor noi proiecte;
- vor valorifica Fondul european de apărare pentru a dezvolta în comun capabilitățile de apărare cibernetică;
- vor dezvolta o înțelegere comună a punerii în aplicare a clauzei de asistență reciprocă în domeniul cibernetic, menținând, în același timp, flexibilitatea acesteia;
- vor dezvolta cerințe de apărare cibernetică de bază pentru infrastructura informațională;
- în măsura în care îmbunătățirea capabilităților de apărare cibernetică depinde de cunoștințele de specialitate din sfera civilă privind securitatea rețelelor și a informațiilor, vor valorifica cunoștințele de specialitate ale ENISA, ale autorităților statelor membre reunite în cadrul grupului de cooperare privind securitatea rețelelor și a informațiilor, precum și ale altor posibile entități la nivelul UE cu cunoștințe de specialitate în securitatea cibernetică civilă.

Statele membre, SEAE/Statul-Major al Uniunii Europene, CESA și AEA:

- vor lua în considerare dezvoltarea formării în domeniul apărării cibernetice în vederea certificării privind grupurile tactice de luptă ale UE.

Comisia, în cooperare cu statele membre:

- va ține seama de securitatea cibernetică în programele de lucru ale Programului european de dezvoltare industrială în domeniul apărării și ale Fondului european de apărare.

2. Sporirea protecției sistemelor de comunicații și informații din cadrul PSAC utilizate de entități ale UE

Fără a aduce atingere rolului Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE) ca structură centrală de coordonare a răspunsului în caz de incidente cibernetice pentru toate instituțiile, organele și agențiile Uniunii și în cadrul normelor relevante privind bugetul Uniunii, SEAE va dezvolta o înțelegere adecvată și autonomă a chestiunilor ce țin de securitate și de apărarea rețelei și va dezvolta propria capacitate de securitate informatică. Aceasta va urmări îmbunătățirea rezilienței rețelelor PSAC ale SEAE, cu accent pe prevenire, detectare, răspunsul în caz de incidente, conștientizarea situației, schimbul de informații și mecanismele de alertă timpurie.

Protecția sistemelor de comunicații și informații ale SEAE și dezvoltarea capacităților în materie de securitate a tehnologiei informației (TI) sunt conduse de către Direcția generală Buget și Administrație (BA) din cadrul SEAE. Statul-Major al Uniunii Europene (EUMS), Direcția de planificare și de gestionare a crizelor (CMPD) și Capacitatea civilă de planificare și conducere (CPCC) vor furniza, de asemenea, sprijin și resurse dedicate suplimentare. Această capacitate în materie de securitate informatică va acoperi atât sistemele clasificate, cât și cele neclasificate și va face parte integrantă din entitățile operaționale existente.

De asemenea, este necesar ca pe parcursul desfășurării misiunilor și operațiilor PSAC să se raționalizeze normele de securitate pentru sistemele de informații furnizate de diferiți actori instituționali din UE. În acest context, ar putea fi luat în considerare un lanț de comandă unificat, cu scopul de a îmbunătăți reziliența rețelelor utilizate pentru PSAC.

Pentru o mai bună coordonare și pentru a consolida protecția și reziliența sistemelor și rețelelor informatice și de comunicații PSAC, în 2017 a fost creat, în cadrul SEAE, un comitet privind guvernanța cibernetică, sub autoritatea secretarului general al SEAE.

SEAE/BA:

- vor consolida capacitatea în materie de securitate informatică din cadrul SEAE, pe baza capacităților și a procedurilor tehnice existente, cu accent pe prevenire, detectare, răspunsul în caz de incidente, conștientizarea situației, schimbul de informații și mecanismul de alertă timpurie. Va fi consolidată în continuare strategia de cooperare cu CERT-UE și cu capabilitățile existente ale UE în materie de securitate cibernetică.

SEAE/BA, împreună cu EUMS, MPCC, CMPD și CPCC:

- vor dezvolta o politică și orientări coerente în materie de securitate informatică, ținând seama totodată de cerințele tehnice pentru apărarea cibernetică în contextul PSAC pentru structuri, misiuni și operații, luând în considerare cadrele și politicile de cooperare existente în cadrul UE pentru a atinge convergența la nivelul normelor, al politicilor și al organizării.

SEAE/Capacitatea unică de analiză a informațiilor (SIAC):

- pe baza structurilor existente, își va consolida capabilitățile în materie de informații și de evaluare a amenințărilor cibernetice pentru a identifica noi riscuri cibernetice și va furniza evaluări periodice ale riscurilor pe baza evaluării strategice a amenințării și informații aproape în timp real în caz de incidente, coordonate între structurile relevante ale UE și puse la dispoziție la diferite niveluri de clasificare.

SEAE/SIAC și CERT-UE:

- vor promova schimbul de informații în timp real în materie de amenințări cibernetice între statele membre și entitățile relevante ale UE. În acest scop, între autoritățile relevante la nivel național și european se vor dezvolta mecanisme de schimb de informații și măsuri de consolidare a încrederii, printr-o abordare voluntară care se bazează pe cooperarea existentă.

SEAE/EUMS și MPCC:

- vor dezvolta și integra în continuare în planificarea la nivel strategic un concept privind apărarea cibernetică pentru misiunile și operațiile militare PSAC;
- vor dezvolta, în cooperare cu comandamentul de operații, o procedură standard de operare în domeniul cibernetic la nivelul operațional generic.

SEAE/CPCC și CMPD:

- vor dezvolta și integra în continuare în planificarea la nivel strategic un concept privind apărarea cibernetică pentru misiunile PSAC civile;
- vor consolida capabilitățile de apărare cibernetică ale misiunilor PSAC civile pe baza infrastructurii existente și promovând standardizarea și armonizarea tehnologiilor utilizate în cadrul misiunilor și operațiilor PSAC, valorificând, atunci când este relevant, cunoștințele specializate ale CERT-UE, ENISA și AEA;
- în cadrul procesului de consolidare a PSAC civile, vor examina, în continuare, posibilitatea acordării de asistență țărilor gazdă de către misiunile PSAC civile în ceea ce privește apărarea cibernetică.

SEAE:

- va dezvolta în continuare cerințele comune pentru misiunile și operațiile PSAC civile și militare;
- va consolida coordonarea apărării cibernetice pentru a pune în aplicare obiective legate de protecția rețelelor utilizate de actori instituționali din UE care sprijină PSAC, bazându-se pe experiențele existente de la nivelul întregii UE;
- va reexamina periodic cerințele în materie de resurse și alte decizii de politică relevante pe baza contextului în schimbare al amenințărilor, în consultare cu statele membre și cu alte instituții ale UE.

3. Promovarea cooperării civil-militare

Spațiul cibernetic este un domeniu în rapidă evoluție, iar evoluțiile tehnologice trebuie consolidate de sisteme de securitate, atât în domeniul civil, cât și în cel militar. În măsura în care este posibil, ar trebui prevăzută coordonarea între domeniul civil și cel militar în cazurile în care evoluții tehnologice similare oferă soluții pentru aplicații civile și militare. În alte cazuri, capabilitățile militare și sistemele de arme sunt atât de specifice încât nu există nicio marjă pentru schimburile cu tehnologiile civile. Fără a aduce atingere organizării și legislației interne ale statelor membre, cooperarea civil-militară în domeniul cibernetic poate fi luată în considerare pentru, printre altele, schimbul de bune practici, mecanismele de schimb de informații și de alertă timpurie, evaluările riscurilor și acțiunile de sensibilizare în ceea ce privește răspunsurile la incidente, precum și pentru formare și exerciții.

Îmbunătățirea securității cibernetice civile este un factor important care contribuie la reziliența generală a securității rețelelor și a informațiilor. Directiva privind securitatea rețelelor și a informațiilor crește gradul de pregătire la nivel național și consolidează cooperarea la nivelul Uniunii între statele membre, atât la nivel strategic, cât și la nivel operațional. Această cooperare include atât autoritățile naționale care supervizează politicile în materie de securitate cibernetică, cât și CERT-urile naționale și CERT-UE. Cooperarea dintre CERT-urile civile și militare ar trebui consolidată ținând cont, în mod corespunzător, de aceste evoluții. Obiectivul noii legi europene privind securitatea cibernetică este de a îmbunătăți reziliența europeană față de atacurile cibernetice și de a oferi un cadru de certificare pentru produsele și serviciile din domeniul securității cibernetice, sporind astfel încrederea în domeniul digital civil.

AEA, Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), Centrul european de combatere a criminalității informatice (EC3) și CERT-UE, împreună cu alte organe și agenții relevante ale UE, în cadrul mandatelor lor respective și fără a se suprapune cu competențele statelor membre, precum și statele membre sunt încurajate să își consolideze în continuare cooperarea în următoarele domenii:

- dezvoltarea unor profiluri de competență comune în materie de securitate cibernetică și de apărare cibernetică, pe baza bunelor practici internaționale și a certificării utilizate de instituțiile, organele și agențiile UE, luând în considerare, de asemenea, standardele de certificare din sectorul privat;
- contribuția la dezvoltarea în continuare și adaptarea standardelor organizaționale și tehnice în materie de securitate cibernetică și de apărare cibernetică din sectorul public în vederea utilizării în sectorul apărării și al securității, acolo unde este necesar, pe baza lucrărilor în curs ale ENISA și AEA;
- stabilirea sau dezvoltarea în continuare a unor mecanisme și modalități de lucru pentru a face schimb de bune practici, în special în materie de educație, formare și exerciții, precum și în materie de cercetare și tehnologie și alte domenii care oferă sinergii civil-militare;
- valorificarea experiențelor existente la nivelul UE în ceea ce privește prevenirea și investigarea cazurilor de criminalitate cibernetică, precum și capabilitățile criminalistice din acest domeniu și utilizarea lor sporită în dezvoltarea capabilităților de apărare cibernetică.

Statele membre, pe bază voluntară:

- vor consolida cooperarea dintre CERT-urile civile și militare între statele membre.

SEAE, Comisia și statele membre:

- vor include apărarea cibernetică în procedurile de gestionare a crizelor și dezastrelor (prin procesul *Blue Print*).

4. Cercetare și tehnologie

Operatorii de servicii de infrastructură și tehnologie a informației și a comunicațiilor (TIC) în scopuri civile și de apărare se confruntă cu provocări de securitate cibernetică similare, ca urmare a cerințelor comune în materie de capacitate tehnologică și operațională. Se preconizează că nevoile comune legate de cercetare și tehnologie și cerințele comune privind sistemele vor îmbunătăți interoperabilitatea sistemelor pe termen lung și vor reduce costurile de dezvoltare a soluțiilor. Pentru a face față numărului tot mai mare de amenințări și vulnerabilități, este necesară realizarea de economii de scară. Aceasta ar trebui, la rândul ei, să faciliteze conservarea și creșterea unei industrii competitive a apărării cibernetice în Europa.

Dezvoltarea de capabilități de apărare cibernetică are o importantă dimensiune de cercetare și tehnologie. În cadrul agendei de cercetare în domeniul apărării cibernetice (CDRA), AEA a furnizat o bază solidă pentru stabilirea priorităților viitoarei finanțări pentru cercetare și tehnologie la nivelul cadrului interguvernamental. Agenda de cercetare strategică ulterioară elaborată în cadrul Grupului de lucru ad-hoc relevant al AEA prevede o stabilire documentată a priorităților în ceea ce privește tehnologiile din domeniul cibernetic necesare în scop militar, identificând în același timp oportunitățile de acțiuni și de investiții în tehnologiile cu dublă utilizare, în contexte fie naționale, fie multinaționale sau care implică finanțare din partea UE.

Este esențială dezvoltarea unor capacități tehnologice în Europa pentru atenuarea amenințărilor și a vulnerabilităților. Industria va rămâne principalul factor determinant pentru tehnologie și inovare în domeniul apărării cibernetice. Criptografia, sistemele integrate securizate, detectarea programelor malware, tehnicile de simulare și vizualizare, protecția rețelelor și a sistemelor de comunicații, tehnologia de identificare și autentificare sunt câteva dintre domeniile care trebuie abordate. De asemenea, este important să se promoveze un lanț de aprovizionare competitiv pentru securitatea cibernetică industrială europeană prin susținerea implicării întreprinderilor mici și mijlocii (IMM-uri).

Asigurarea faptului că Europa este în măsură să țină pasul cu concurenți internaționali în materie de capabilități tehnologice cibernetice depinde, de asemenea, de capacitatea noastră de a stimula inovarea revoluționară, prin instrumente naționale, dar și ale UE, cum ar fi Consiliul european pentru inovare.

Pentru a facilita cooperarea civil-militară în materie de dezvoltare de capabilități de apărare cibernetică, pentru a consolida baza industrială și tehnologică de apărare europeană[10] și pentru a contribui la autonomia strategică a UE și în domeniul cibernetic, atunci când și acolo unde va fi necesar, precum și împreună cu parteneri, acolo unde va fi posibil**,**

AEA, Comisia și statele membre:

- vor urmări sinergii ale eforturilor în materie de cercetare și tehnologie din sectorul militar cu programele de cercetare și dezvoltare civile, în special cele privind inovațiile revoluționare, și vor ține seama de dimensiunea securității și apărării cibernetice în cadrul punerii în aplicare a Acțiunii pregătitoare privind cercetarea în materie de apărare;
- vor disemina agendele de cercetare în materie de securitate cibernetică (de exemplu agenda de cercetare strategică privind securitatea cibernetică a Agenției Europene de Apărare), precum și foile de parcurs și acțiunile care vor rezulta din acestea; în acest scop, va fi elaborată o agendă de cercetare transsectorială în materie de apărare cibernetică, în strânsă colaborare cu Comisia și cu statele membre;
- vor contribui la îmbunătățirea integrării dimensiunilor de securitate cibernetică și apărare cibernetică în programele care au o dimensiune de securitate și apărare cu dublă utilizare, de exemplu Programul de cercetare privind managementul traficului aerian în cerul unic european (SESAR).

[10] Comunicarea „Către un sector al apărării și al securității mai competitiv și mai eficient”, COM (2013) 542.

Comisia:

- va avea în vedere crearea unui centru de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a unei rețele de centre naționale de coordonare, pentru a sprijini capacitățile tehnologice și industriale în materie de securitate cibernetică și pentru a îmbunătăți competitivitatea industriei securității cibernetice a Uniunii, asigurând complementaritatea și evitând suprapunerile în cadrul Rețelei centrelor de competență în materie de securitate cibernetică și cu alte agenții ale UE. Centrul ar trebui, printre altele, să consolideze cooperarea dintre tehnologiile și aplicațiile civile și de apărare, în strânsă colaborare și în deplină complementaritate cu Agenția Europeană de Apărare în domeniul apărării cibernetice;
- va sprijini dezvoltarea unor ecosisteme industriale și a unor clustere de inovare care să acopere întregul lanț valoric de securitate pe baza cunoștințelor academice, a inovării IMM-urilor și a producției industriale.

Comisia, în cooperare cu statele membre:

- va analiza aspecte referitoare la apărarea cibernetică ale cererilor din cadrul Acțiunii pregătitoare privind cercetarea în materie de apărare;
- va lua în considerare apărarea cibernetică în temele care vor fi acoperite de Fondul european de apărare;
- va sprijini coerența politicilor UE pentru a garanta că aspectele politice și tehnice ale protecției cibernetice la nivelul UE rămân în avangarda inovării tehnologice și sunt armonizate în întreaga UE (capacitatea de analiză și evaluare a amenințărilor cibernetice, inițiativele privind „securitatea de la stadiul conceperii”, gestionarea dependenței pentru accesul la tehnologie etc.).

5. Îmbunătățirea oportunităților de educație, de formare și de exerciții

În vederea creșterii gradului de pregătire pentru răspunsul la amenințările cibernetice și a dezvoltării unei culturi comune de apărare cibernetică în întreaga UE, de care să beneficieze și misiunile și operațiile UE, este necesar să se îmbunătățească și să se extindă oportunitățile de formare în materie de apărare cibernetică. Este esențial ca bugetele pentru educație și formare să fie utilizate eficient, oferind în același timp cea mai bună calitate posibilă. Gruparea și utilizarea în comun a activităților de educație și formare în materie de apărare cibernetică la nivel european vor fi de o importanță majoră.

Colegiul European de Securitate și Apărare (CESA), SEAE, AEA, Comisia și statele membre:

- pe baza analizei AEA a nevoilor de formare în materie de apărare cibernetică și a experienței dobândite de CESA în domeniul formării pentru securitatea cibernetică, vor stabili activități de formare și educație în cadrul PSAC pentru diferite categorii de public, inclusiv SEAE, personalul din misiunile și operațiile PSAC și funcționarii statelor membre, care ar trebui să abordeze și problemele legate de fidelizarea personalului calificat pe termen scurt, mediu și lung;
- vor propune instituirea unui dialog în domeniul apărării cibernetice privind standardele de formare și certificarea cu statele membre, instituțiile UE, țări terțe și alte organizații internaționale, precum și cu sectorul privat;
- vor stabili contacte cu furnizori de formare din sectorul privat european, precum și cu instituțiile academice, pentru a îmbunătăți competențele și aptitudinile personalului implicat în misiunile și operațiile PSAC.

CESA:

- va dezvolta în continuare platforma de educație, formare, evaluare și exerciții în domeniul cibernetic stabilită în cadrul CESA (platforma EFEE în domeniul cibernetic);
- va crea sinergii cu programele de formare ale altor părți interesate, precum ENISA, Europol, Colegiul European de Poliție (CEPOL) și Centrul de excelență pentru cooperare în domeniul apărării cibernetice al NATO;
- va analiza posibilitatea unor programe de formare comune CESA-NATO în domeniul apărării cibernetice, deschise tuturor statelor membre ale UE, în vederea promovării unei culturi comune de apărare cibernetică.

Comisia:

- va evalua opțiunile pentru extinderea oportunităților de formare și de educație din statele membre identificate de platforma EFEE în domeniul cibernetic.

AEA:

- va dezvolta noi cursuri ale AEA în colaborare cu CESA pentru a răspunde cerințelor de educație, de formare și de exerciții în materie de apărare cibernetică ale statelor membre;
- va sprijini platforma EFEE în domeniul cibernetic, printre altele prin integrarea progresivă a modulelor de educație, de formare și de exerciții dezvoltate în cadrul AEA.

SEAE și statele membre:

- vor urma mecanismele de certificare ale CESA stabilite pentru programele de formare, în strânsă cooperare cu serviciile relevante din cadrul instituțiilor, al organelor și al agențiilor UE, pe baza standardelor și a cunoștințelor existente; vor analiza posibilitatea de a crea module specifice ciberneticii în cadrul inițiativei Erasmus în domeniul militar.

Este necesară îmbunătățirea oportunităților de exerciții în domeniul apărării cibernetice pentru actorii PSAC militari și civili. Exercițiile comune reprezintă un instrument de dezvoltare a cunoștințelor și a înțelegerii comune privind apărarea cibernetică. Acest lucru va permite forțelor naționale să își îmbunătățească gradul de pregătire pentru a opera într-un mediu multinațional. Desfășurarea unor exerciții comune de apărare cibernetică va consolida, de asemenea, interoperabilitatea și încrederea.

SEAE, AEA, CERT-UE și statele membre se vor axa pe promovarea elementelor de apărare cibernetică în contextul PSAC și al altor exerciții:

- integrarea unei dimensiuni de apărare cibernetică în scenariile de exerciții existente pentru *MILEX* și *MULTILAYER*;
- organizarea periodică de exerciții strategice/politice precum *CYBRID 2017*, în coordonare cu exercițiul paralel și coordonat (PACE) condus de UE, și de exerciții tehnico-operaționale precum *DEFNET*;
- dezvoltarea, după caz, a unui exercițiu dedicat de apărare cibernetică în cadrul PSAC la nivelul UE și analizarea posibilității de coordonare cu exerciții paneuropene în domeniul ciberneticii precum *Cyber Europe*, organizat de ENISA;
- continuarea participării la alte exerciții multinaționale de apărare cibernetică, cum ar fi *Locked Shields*;
- invitarea la exerciții a partenerilor internaționali relevanți, precum NATO, în conformitate cu cadrul de politici ale UE în materie de exerciții;
- organizarea de exerciții periodice pe baza setului de instrumente pentru diplomația cibernetică, în care statele membre ale UE pot exersa răspunsul la activitățile cibernetice răuvoitoare.

6. Consolidarea cooperării cu parteneri internaționali relevanți

În cadrul cooperării internaționale, este necesar să se asigure un dialog cu partenerii internaționali, în special NATO și alte organizații internaționale, în scopul de a contribui la dezvoltarea unor capacități de apărare cibernetică eficace. Ar trebui urmărită o implicare sporită în activitatea desfășurată în prezent în cadrul Organizației pentru Securitate și Cooperare în Europa (OSCE) și al Organizației Națiunilor Unite (ONU), în vederea propunerii unui cadru strategic pentru prevenirea conflictelor, pentru cooperare și pentru stabilitate în spațiul cibernetic.

Există o voință politică în UE de a se continua cooperarea cu NATO în materie de apărare cibernetică în ceea ce privește dezvoltarea unor capabilități de apărare cibernetică robuste și reziliente, astfel cum se prevede în Declarația comună semnată de președintele Consiliului European, de președintele Comisiei Europene și de secretarul general al Organizației Tratatului Atlanticului de Nord la Varșovia la 8 iulie 2016. Consultările periodice la nivel de personal, informările încrucișate, precum și eventualele reuniuni între Grupul politico-militar și comitetele NATO relevante vor contribui la evitarea suprapunerilor inutile și vor asigura coerența și complementaritatea eforturilor, în concordanță cu cadrul menționat anterior.

SEAE și AEA, împreună cu statele membre, vor dezvolta în continuare cooperarea în materie de apărare cibernetică dintre UE și NATO, cu respectarea corespunzătoare a cadrului instituțional și a autonomiei decizionale a acestor organizații respective:

- vor intensifica activitățile în curs în cadrul punerii în aplicare a Declarației comune a președintelui Consiliului European, președintelui Comisiei Europene și secretarului general al Organizației Tratatului Atlanticului de Nord;
- vor face schimb de bune practici cu privire la gestionarea crizelor, precum și în materie de apărare cibernetică ale misiunilor și operațiilor militare și civile;
- vor depune eforturi pentru asigurarea coerenței rezultatelor în cadrul dezvoltării cerințelor în materie de capabilități de apărare cibernetică acolo unde acestea se suprapun, în special în cadrul dezvoltării de capabilități de apărare cibernetică pe termen lung;
- utilizarea în continuare a cadrului de cooperare al AEA cu Centrul de excelență pentru cooperare în domeniul apărării cibernetice al NATO ca platformă inițială pentru o colaborare sporită în proiectele de apărare cibernetică multinaționale, pe baza unor evaluări corespunzătoare.

CESA, SEAE și AEA:

- vor consolida cooperarea privind conceptele pentru formarea, educația și exercițiile în materie de apărare cibernetică;
- vor asigura participarea reciprocă a personalului la exerciții, în conformitate cu cadrul convenit.

CERT-UE:

- va exploata în continuare acordul tehnic dintre CERT-UE și NCIRC (Capacitatea de răspuns la incidente informatice a NATO), în vederea îmbunătățirii gradului de conștientizare a situației, a schimbului de informații și a mecanismelor de alertă timpurie, precum și în vederea anticipării amenințărilor care ar putea afecta ambele organizații.

În ceea ce privește alte organizații internaționale și parteneri internaționali relevanți ai UE, SEAE și statele membre, după caz:

- vor urmări evoluțiile strategice și vor organiza consultări pe marginea unor chestiuni legate de apărarea cibernetică cu partenerii internaționali (organizații internaționale și țări terțe);
- vor analiza posibilități de cooperare în chestiuni referitoare la apărarea cibernetică, inclusiv cu țările terțe care participă la misiuni și operații PSAC;
- vor promova în cadrul organizațiilor internaționale relevante, în special ONU, OSCE și Forumul regional ASEAN, aplicarea în spațiul cibernetic a dreptului internațional existent, în special a Cartei ONU în deplinătatea sa, elaborarea și punerea în aplicare a unor norme universale, fără caracter obligatoriu, referitoare la un comportament responsabil din partea statelor și măsuri regionale de consolidare a încrederii (CBM) între state în vederea sporirii transparenței și a reducerii riscului de percepere greșită a comportamentului statal.

Comisia și SEAE:

- acolo unde va fi relevant, vor sprijini consolidarea capabilităților cibernetice pentru partenerii UE prin intermediul Instrumentului care contribuie la stabilitate și pace (IcSP) modificat.

Acțiuni ulterioare

În cadrul coordonării SEAE a punerii în aplicare a CDPF, SEAE/AEA/Comisia ar trebui să prezinte un raport intermediar anual, care să includă cele șase domenii menționate mai sus, în cadrul Grupului politico-militar, cu participarea membrilor Grupului de lucru orizontal pentru chestiuni cibernetice, precum și în cadrul Comitetului politic și de securitate, pentru a evalua punerea în aplicare a CDPF. De asemenea, o dată la șase luni se va face o prezentare orală.

Este esențial ca, pe măsură ce amenințarea cibernetică evoluează, să se identifice noi cerințe de apărare cibernetică, care să fie apoi incluse în cadrul de politici pentru apărarea cibernetică. Următoarea revizuire a CDPF ar trebui prezentată cel târziu până la jumătatea anului 2022, în urma unor consultări strânse cu statele membre.