COMISIA EUROPEANĂ

ÎNALTUL REPREZENTANT AL UNIUNII PENTRU AFACERI EXTERNE ȘI POLITICA DE SECURITATE

Bruxelles, 13.9.2017
JOIN(2017) 450 final

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN ŞI CONSILIU

Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE

1. INTRODUCERE

Securitatea cibernetică este esențială atât pentru prosperitatea noastră, cât și pentru siguranța noastră. Întrucât viața noastră cotidiană și economiile noastre depind tot mai mult de tehnologiile digitale, suntem din ce în ce mai expuși. Incidentele de securitate cibernetică se diversifică în ceea ce privește atât entitatea responsabilă, cât și scopul urmărit. Activitățile cibernetice răuvoitoare ne amenință nu numai economiile și realizarea unei piețe unice digitale, ci și funcționarea democrațiilor, libertatea și valorile noastre. Securitatea noastră viitoare depinde de transformarea capacității noastre de a proteja UE împotriva amenințărilor cibernetice: atât infrastructura civilă, cât și capacitatea militară se bazează pe sisteme digitale securizate. Acest lucru a fost recunoscut în cadrul Consiliului European din iunie 2017[1], precum și în Strategia globală pentru politica externă și de securitate a Uniunii Europene[2].

Riscurile cresc exponențial. Studiile sugerează că impactul economic al criminalității cibernetice a crescut de cinci ori în perioada 2013 - 2017 și ar putea crește de încă patru ori până în 2019[3]. Programele de șantaj digital (*ransomware)*[4] s-au dezvoltat în special, cele mai recente atacuri[5] reflectând o creștere dramatică a activităților de criminalitate cibernetică. Cu toate acestea, programele de șantaj digital nu sunt singura amenințare.

Amenințările cibernetice vin atât din partea actorilor statali, cât și din partea actorilor nestatali: acestea sunt, în general, motivate de profit, însă pot fi, de asemenea, politice și strategice. Amenințarea infracțională este intensificată prin estomparea graniței dintre criminalitatea cibernetică și criminalitatea „tradițională", întrucât infractorii utilizează internetul atât ca o modalitate de a-și intensifica activitățile, cât și ca o sursă pentru a găsi noi metode și instrumente în scopul de a săvârși infracțiuni[6]. Cu toate acestea, în marea majoritate a cazurilor, șansele de a identifica infractorul sunt minime, iar șansele de a-l urmări penal sunt chiar mai mici.

În același timp, actorii statali își îndeplinesc din ce în ce mai mult obiectivele geopolitice nu numai prin instrumentele tradiționale, cum ar fi forța armată, ci și prin intermediul unor instrumente cibernetice mai discrete, care includ influențarea proceselor democratice la nivel intern. Utilizarea spațiului cibernetic ca un câmp de război, fie în întregime, fie ca parte a unei abordări hibride, este recunoscută în prezent la scară largă. Campaniile de dezinformare, știrile false și operațiunile cibernetice care vizează infrastructurile critice sunt din ce în ce mai răspândite și necesită un răspuns. Din acest motiv, în documentul său de reflecție privind viitorul apărării europene[7], Comisia a subliniat importanța cooperării în domeniul apărării cibernetice.

Dacă nu ne vom îmbunătăți în mod considerabil securitatea cibernetică, atunci riscul va crește proporțional cu transformarea digitală. Zeci de miliarde de dispozitive care fac parte din

---

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

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

3 A se vedea, de exemplu, McAfee & Centrul pentru studii strategice și internaționale *Net losses: Estimating the Global Cost of Cybercrime* (Pierderile nete: estimarea costului global al criminalității cibernetice), 2014.

4 „Programul de șantaj digital" este un tip de program malware care împiedică sau limitează accesul utilizatorilor la sistemul lor, fie prin blocarea ecranului sistemului, fie prin blocarea fișierelor utilizatorilor, până când se plătește o răscumpărare.

5 În mai 2017, atacul cibernetic „WannaCry" care a utilizat un program de șantaj digital a afectat peste 400 000 de calculatoare din peste 150 de țări. O lună mai târziu, atacul cibernetic „Petya", care a utilizat un program de șantaj digital, a lovit Ucraina și o serie de societăți din întreaga lume.

6 Europol, *Serious and Organised Crime Threat Assessment* (Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată), 2017.

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

„internetul obiectelor” vor fi conectate la internet până în 2020, însă securitatea cibernetică nu reprezintă încă o prioritate în procesul de concepere a acestora[8]. Incapacitatea de a proteja dispozitivele care vor controla rețelele electrice, mașinile și rețelele de transport, fabricile, finanțele, spitalele și locuințele noastre ar putea avea consecințe devastatoare și ar putea afecta profund încrederea consumatorilor în tehnologiile emergente. Riscul de atacuri motivate politic asupra țintelor civile și deficiențele în ceea ce privește apărarea militară împotriva criminalității cibernetice sporesc și mai mult pericolul.

Abordarea stabilită în prezenta comunicare comună va plasa UE într-o poziție mai bună pentru a face față acestor amenințări. Aceasta ar consolida o mai mare reziliență și autonomie strategică, contribuind la sporirea capacităților în materie de tehnologie și de competențe, precum și la construirea unei piețe unice puternice. Acest lucru necesită structuri adecvate care să consolideze securitatea cibernetică și să reacționeze în caz de necesitate, cu implicarea deplină a tuturor actorilor principali. De asemenea, abordarea ar descuraja cu mai mare succes atacurile cibernetice, prin intensificarea activităților pentru a detecta, a depista și a trage la răspundere persoanele responsabile de atacuri. Aceasta ar recunoaște, de asemenea, dimensiunea globală a securității cibernetice prin dezvoltarea cooperării internaționale ca o platformă pentru poziția de lider a UE în ceea ce privește securitatea cibernetică. Aceste măsuri se bazează pe abordările privind piața unică digitală, strategia globală, Agenda europeană privind securitatea[9], Cadrul comun privind contracararea amenințărilor hibride[10] și Comunicarea privind lansarea Fondului european de apărare[1112].

UE abordează deja în activitatea sa multe dintre aceste aspecte: este momentul de a reuni diversele fluxuri de activități. În 2013, UE a stabilit o strategie de securitate cibernetică prin care lansează o serie de fluxuri de activități principale în vederea îmbunătățirii rezilienței cibernetice[13]. Principalele sale obiective și principii, de a promova un ecosistem cibernetic fiabil, sigur și deschis, rămân valabile. Cu toate acestea, amenințările aflate în continuă evoluție și intensificare solicită luarea mai multor măsuri pentru a rezista în fața atacurilor și a le descuraja în viitor[14].

UE este în măsură să abordeze securitatea cibernetică, având în vedere domeniul de aplicare a politicilor sale și instrumentele, structurile și capacitățile de care dispune. În timp ce statele membre rămân responsabile de securitatea națională, amploarea și caracterul transfrontalier al amenințării reprezintă argumente puternice pentru ca acțiunea UE să furnizeze stimulente și sprijin statelor membre pentru a dezvolta și a menține capacități naționale sporite și îmbunătățite în domeniul securității cibernetice, construind, în același timp, capacități la nivelul UE. Această abordare are scopul de a mobiliza toți actorii – UE, statele membre, industria și cetățenii – în scopul de a acorda securității cibernetice prioritatea necesară pentru a consolida reziliența și a furniza un răspuns mai bun din partea UE la atacurile cibernetice.

---

8 Soluții IDC și TXT (2014), SMART 2013/0037 *Cloud and IoT combination* (Combinația cloud și internetul obiectelor), studiu efectuat pentru Comisia Europeană.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 De asemenea, abordarea este susținută de consilierea științifică independentă furnizată de mecanismul de consiliere științifică format din grupul la nivel înalt de consilieri științifici al Comisiei Europene (a se vedea referințele de mai jos).

13 JOIN(2013) 1 final. O evaluare a strategiei este disponibilă în documentul de lucru al serviciilor Comisiei SWD (2017) 295.

14 Cu excepția cazului în care se precizează altfel, propunerile din prezenta Comunicare sunt neutre din punct de vedere bugetar. Orice inițiativă care are implicații bugetare va urma în mod corespunzător procedurile bugetare anuale și nu poate aduce atingere următorului cadru financiar multianual post-2020.

Aceasta va introduce măsuri concrete pentru a contribui la depistarea și investigarea oricăror forme de incidente cibernetice împotriva UE și împotriva statelor sale membre, precum și pentru a răspunde în mod adecvat, inclusiv prin urmărirea penală a infractorilor. Abordarea va permite luarea unor măsuri de către UE la nivel extern pentru a promova în mod eficace securitatea cibernetică la nivel mondial. Rezultatul va fi o trecere pentru UE de la o abordare reactivă la una proactivă pentru protejarea prosperității, a societății și a valorilor europene, precum și a drepturilor și libertăților fundamentale, răspunzând atât la amenințările existente, cât și la cele viitoare.

2. CONSOLIDAREA REZILIENȚEI UE LA ATACURILE CIBERNETICE

O reziliență cibernetică puternică necesită o abordare cuprinzătoare și colectivă. Aceasta necesită structuri mai solide și mai eficace pentru a promova securitatea cibernetică și a răspunde la atacurile cibernetice în statele membre, precum și la nivelul instituțiilor, agențiilor și organismelor UE. De asemenea, aceasta necesită o abordare mai cuprinzătoare și trans-sectorială privind consolidarea rezilienței cibernetice și a autonomiei strategice, cu o piață unică puternică, progrese majore în ceea ce privește capacitatea tehnologică a UE și un număr mult mai mare de experți calificați. În centrul acestei abordări se află o mai largă acceptare a faptului că securitatea cibernetică este o provocare societală comună, astfel încât este necesară implicarea pe mai multe niveluri a guvernului, a economiei și a societății.

2.1 Consolidarea Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) îndeplinește un rol esențial în consolidarea rezilienței cibernetice și a reacției la atacurile cibernetice, însă aceasta este limitată de mandatul său actual. Prin urmare, Comisia prezintă o propunere de reformă ambițioasă, care include un **mandat permanent pentru agenție**[15]. Aceasta va asigura că ENISA poate oferi sprijin statelor membre, instituțiilor UE și întreprinderilor din domeniile-cheie, inclusiv punerea în aplicare a Directivei privind securitatea rețelelor și a sistemelor informatice[16] („Directiva NIS") și a cadrului de certificare propus în materie de securitate cibernetică.

ENISA reformată va avea un puternic rol de consiliere cu privire la elaborarea și punerea în aplicare a politicilor, inclusiv prin promovarea coerenței între inițiativele sectoriale și Directiva NIS și prin sprijinirea instituirii centrelor de schimb și analiză de informații în sectoare critice. ENISA va viza obiective tot mai ambițioase și va îmbunătăți pregătirea la nivel european prin organizarea de exerciții paneuropene anuale privind securitatea cibernetică care combină răspunsul la diferite niveluri. De asemenea, aceasta va sprijini elaborarea politicii UE privind certificarea securității cibernetice a tehnologiei informației și comunicațiilor (TIC) și va îndeplini un rol important în intensificarea cooperării operaționale și a gestionării crizelor la nivelul UE. De asemenea, agenția va constitui un punct de contact pentru informații și cunoștințe în comunitatea din domeniul securității cibernetice.

O înțelegere rapidă și comună a amenințărilor și incidentelor pe măsură ce apar acestea reprezintă o condiție prealabilă pentru a decide dacă este necesară o măsură comună de atenuare sau de răspuns sprijinită de UE. Un astfel de schimb de informații necesită implicarea tuturor actorilor relevanți – organismele și agențiile UE, precum și statele membre

[15] COM(2017) 477.

[16] 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.

– la nivel tehnic, operațional și strategic. ENISA, în colaborare cu organismele competente ale statelor membre și la nivelul UE, în special rețeaua de echipe de intervenție în caz de incidente de securitate cibernetică[17], CERT-EU, Europol și Centrul de analiză a informațiilor al UE (INTCEN), vor contribui, de asemenea, la cunoașterea situației existente la nivelul UE. Aceasta poate contribui la informațiile cu privire la amenințări și la procesul de elaborare a politicilor în contextul monitorizării periodice a peisajului de amenințări și al unei cooperări operaționale eficace, precum și ca răspuns la incidentele transfrontaliere de mare amploare.

2.2 Către o piață unică a securității cibernetice

Creșterea pieței securității cibernetice în UE – în ceea ce privește produsele, serviciile și procesele – este împiedicată în mai multe moduri. Un aspect fundamental îl reprezintă lipsa unor sisteme de certificare în materie de securitate cibernetică recunoscute la nivelul UE în vederea elaborării unor standarde mai ridicate în materie de reziliență pentru produse și a menținerii încrederii pieței pe întreg teritoriul UE. Prin urmare, Comisia înaintează o propunere de instituire a unui **cadru de certificare în materie de securitate cibernetică la nivelul UE**[18]. Cadrul ar stabili procedura pentru crearea unor sisteme de certificare în materie de securitate cibernetică la nivelul UE, vizând produse, servicii și/sau sisteme, care să adapteze nivelul de asigurare la utilizarea implicată (fie că este vorba despre infrastructuri critice sau dispozitive pentru consumatori)[19]. Acesta ar aduce avantaje clare pentru întreprinderi, eliminând necesitatea de a trece prin mai multe procese de certificare în cazul activităților transfrontaliere și reducând astfel costurile administrative și financiare. Utilizarea de sisteme elaborate în temeiul prezentului cadru ar contribui, de asemenea, la consolidarea încrederii consumatorilor, prin intermediul unui certificat de conformitate care să informeze și să ofere asigurări cumpărătorilor și utilizatorilor cu privire la securitatea produselor și a serviciilor pe care le cumpără și le utilizează. Aceasta ar face ca standardele ridicate în materie de securitate cibernetică să devină o sursă de avantaj concurențial. Rezultatul ar consolida reziliența sporită, întrucât produsele și serviciile TIC ar fi evaluate în mod oficial pe baza unui set definit de standarde în materie de securitate cibernetică, care ar putea fi elaborate în strânsă legătură cu activitățile în curs privind standardele TIC[20].

Sistemele cadrului ar urma să fie voluntare și nu ar crea obligații de reglementare imediate vânzătorilor sau furnizorilor de servicii. Sistemele nu ar contraveni cerințelor legale aplicabile, cum ar fi legislația UE în materie de protecție a datelor.

De îndată ce cadrul este stabilit, Comisia va invita părțile interesate să se concentreze pe trei domenii prioritare:

- securitatea în aplicații critice sau cu risc ridicat[21]: sistemele de care depindem în activitățile noastre cotidiene, de la autoturismele noastre la echipamentul din fabrici, de la cel mai mari sisteme, cum ar fi avioanele sau centralele electrice, la cele mai mici sisteme, cum ar fi dispozitivele medicale, care devin din ce în ce mai digitale și interconectate. Prin urmare, componentele TIC esențiale din astfel de produse și sisteme ar necesita evaluări riguroase de securitate.

---

[17] Astfel cum se prevede la articolul 9 din Directiva NIS.

[18] COM(2017) 477.

[19] Un nivel de asigurare indică gradul de rigurozitate al evaluării de securitate și este proporțional, în general, cu nivelul de risc asociat acestor domenii de aplicare sau funcții (și anume, un nivel de asigurare mai ridicat necesar pentru produsele sau serviciile TIC utilizate în domeniile de aplicare sau funcțiile cu grad ridicat de risc).

[20] COM(2016) 176.

[21] Cu excepția cazului în care certificarea obligatorie sau voluntară este reglementată de alte acte ale Uniunii.

- securitatea cibernetică pentru produsele digitale, rețelele, sistemele și serviciile utilizate la scară largă de sectorul public și privat pentru a se apăra împotriva atacurilor și a aplica obligațiile de reglementare[22] – cum ar fi criptarea e-mailurilor, dispozitive de tip firewall și rețele private virtuale; este esențial ca utilizarea răspândită a unor astfel de instrumente să nu conducă la noi surse de risc sau noi vulnerabilități.

- utilizarea metodelor de tip „securitate din stadiul conceperii” pentru dispozitivele digitale interconectate de larg consum cu costuri reduse care alcătuiesc internetul obiectelor: sistemele prevăzute de cadru ar putea fi utilizate pentru a semnala că produsele sunt dezvoltate cu ajutorul celor mai recente metodele de dezvoltare securizate, că au făcut obiectul unor teste de securitate adecvate și că vânzătorii s-au angajat să își actualizeze programele informatice în cazul unor amenințări sau vulnerabilități nou-descoperite.

Aceste priorități ar trebui să aibă în vedere, în special, evoluția peisajului de amenințări la adresa securității cibernetice, precum și importanța unor servicii esențiale precum transportul, furnizarea de energie, serviciile de sănătate, serviciile bancare, infrastructurile piețelor financiare, apa potabilă și infrastructura digitală[23].

În timp ce nu se poate garanta că un produs, un serviciu sau un sistem TIC este „100 %” sigur, există mai multe defecte bine cunoscute și bine documentate în proiectarea produselor TIC care pot fi exploatate pentru atacuri. O abordare de tip „securitate din stadiul conceperii” adoptată de producătorii de dispozitive conectate, programe și echipamente informatice ar garanta faptul că securitatea cibernetică este luată în considerare înainte de punerea pe piață a noilor produse. Această abordare ar putea fi parte a „obligației de diligență”, care urmează a fi elaborată împreună cu industria și care ar putea reduce vulnerabilitățile programelor informatice/produselor prin aplicarea unei serii de metode de la etapa de proiectare la etapa de testare și de verificare, inclusiv verificarea oficială, dacă este cazul, întreținerea pe termen lung și utilizarea unor procese de dezvoltare securizate de-a lungul ciclului de viață, precum și actualizările și corecțiile pe parcurs pentru a aborda vulnerabilitățile nedescoperite anterior și actualizări și reparații rapide[24]. De asemenea, această abordare ar spori încrederea consumatorilor în produsele digitale.

În plus, trebuie să fie recunoscut rolul important al cercetătorilor terți în domeniul securității în descoperirea vulnerabilităților din produsele și serviciile existente și ar trebui create condiții care să permită divulgarea coordonată a vulnerabilității[25] în toate statele membre, pe baza celor mai bune practici[26] și a standardelor relevante[27].

În același timp, **anumite sectoare** se confruntă cu probleme specifice și ar trebui să fie încurajate să își dezvolte propria abordare. În acest mod, strategiile generale privind

---

[22] De exemplu, Directiva (UE) 2016/1148, Regulamentul (UE) 2016/679, Directiva (UE) 2015/2366 și alte acte legislative propuse, cum ar fi Codul european al comunicațiilor electronice, prevăd fiecare ca organizațiile să pună în aplicare măsuri de securitate adecvate pentru a aborda riscurile de securitate cibernetică relevante.

[23] Sectoarele care intră în domeniul de aplicare a Directivei 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

[24] Securitatea cibernetică pe piața unică digitală europeană, grupul la nivel înalt de consilieri științifici, martie 2017

[25] Divulgarea coordonată a vulnerabilității este o formă de cooperare care facilitează și permite cercetătorilor în domeniul securității să raporteze vulnerabilitățile către proprietarul sau vânzătorul de sistem de informații, oferind organizației posibilitatea de a determina și a remedia vulnerabilitatea în mod corect și în timp util înainte ca informațiile detaliate privind vulnerabilitatea să fie divulgate unor părți terțe sau publicului.

[26] De exemplu, Ghidul de bune practici privind divulgarea vulnerabilității. De la provocări la recomandări, ENISA, 2016

[27] ISO/IEC 29147:2014, Tehnologia informației -- Tehnici de securitate -- Divulgarea vulnerabilității.

securitatea cibernetică ar fi completate de strategii privind securitatea cibernetică la nivel de sector în domenii precum serviciile financiare[28], sectorul energiei electrice, transporturi și servicii de sănătate[29].

Comisia a evidențiat deja probleme specifice referitoare la **răspundere** generate de noile tehnologii digitale[30] iar activitățile sunt curs de desfășurare pentru a analiza implicațiile; următoarele etape vor fi finalizate până în iunie 2018. Securitatea cibernetică ridică probleme legate de atribuirea daunelor pentru întreprinderi și lanțuri de aprovizionare, iar incapacitatea de a soluționa aceste probleme va constitui un obstacol în calea dezvoltării unei piețe unice puternice pentru produsese și serviciile din domeniul securității cibernetice.

În cele din urmă, dezvoltarea pieței unice a UE depinde, de asemenea, de includerea securității cibernetice în politica privind comerțul și investițiile. Efectul achizițiilor străine asupra tehnologiilor critice – printre care securitatea cibernetică este un exemplu important – este un aspect esențial al cadrului privind **verificarea investițiilor străine directe în cadrul Uniunii Europene**[31], care urmărește să permită verificarea investițiilor din țările terțe pe motive de siguranță și ordine publică. În aceeași ordine de idei, cerințele în materie de securitate cibernetică au creat deja bariere comerciale pentru bunurile și serviciile UE din sectoarele importante într-o serie de economii ale țărilor terțe. Cadrul UE de certificare în materie de securitate cibernetică va consolida și mai mult poziția Europei pe plan internațional și ar trebui să fie completat de eforturi continue în vederea elaborării unor standarde globale de înaltă securitate și de acorduri de recunoaștere reciprocă.

2.3 Punerea în aplicare pe deplin a Directivei privind securitatea rețelelor și a sistemelor informatice

Având în vedere faptul că principalele instrumente pentru combaterea securității cibernetice în prezent se regăsesc la nivel național, UE a recunoscut necesitatea de crea standarde la un nivel mai înalt. Incidentele de securitate cibernetică la scară largă afectează rareori numai un singur stat membru din cauza naturii din ce în ce mai globalizate, dependente de mediul digital și interconectate a unor sectoare-cheie, cum ar fi sectorul bancar, al energiei și al transporturilor.

Directiva privind securitatea rețelelor și a sistemelor informatice („Directiva NIS”) este primul act legislativ în materie de securitate cibernetică la nivelul UE[32]. Aceasta este concepută pentru a consolida reziliența prin îmbunătățirea capacităților naționale în domeniul securității cibernetice, prin încurajarea unei mai bune cooperări între statele membre și prin impunerea obligației ca întreprinderile din sectoarele economice importante să adopte practici eficace de gestionare a riscurilor și să raporteze autorităților naționale incidentele grave. Aceste obligații se aplică, de asemenea, pentru trei tipuri de furnizori de servicii esențiale de acces la internet: cloud computing, motoare de căutare și piețe online. Acestea vizează o abordare mai sistematică și mai solidă și un flux mai bun de informații.

Punerea în aplicare pe deplin a directivei de către toate statele membre până în mai 2018 este esențială pentru reziliența cibernetică a UE. Procesul este sprijinit de activitățile colective

[28] Activitățile viitoare ale Comisiei în legătură cu tehnologiile financiare vor viza securitatea cibernetică pentru sectorul financiar.

[29] În sectorul energetic, de exemplu, combinarea tehnologiilor informației foarte vechi cu tehnologiile de vârf, în special cerințele în timp real ale rețelei electrice.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] 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.

desfășurate de statele membre, care vor conduce, până în toamna anului 2017, la elaborarea unor orientări pentru a sprijini o punere în aplicare mai armonizată, în special în ceea ce privește operatorii de servicii esențiale. De asemenea, Comisia emite o comunicare[33] ca parte a acestui pachet de măsuri în materie de securitate cibernetică, pentru a sprijini eforturile acestora prin prezentarea celor mai bune practici din statele membre relevante pentru punerea în aplicare a directivei și prin furnizarea de orientări privind modul în care directiva ar trebui să funcționeze în practică.

Un domeniu în care directiva va trebui să fie completată este fluxul de informații. De exemplu, directiva vizează numai anumite sectoare strategice importante – însă, în mod logic, o abordare similară adoptată de toate părțile interesate afectate de atacurile cibernetice ar fi necesară pentru a exista o evaluare sistematică a vulnerabilităților și a punctelor de intrare pentru atacatorii cibernetici. În plus, cooperarea și schimbul de informații între sectorul public și privat se confruntă cu o serie de obstacole. Guvernele și autoritățile publice sunt reticente în a împărtăși informații privind securitatea cibernetică din cauza riscului de compromitere a securității naționale sau a competitivității. Întreprinderile private sunt reticente în a efectua schimburi de informații cu privire la vulnerabilitățile lor cibernetice și pierderile rezultate, de teamă de a compromite informațiile comerciale sensibile, de a-și risca reputația sau de a risca să încalce normele de protecție a datelor[34]. Trebuie să fie consolidată încrederea pentru parteneriatele dintre sectorul public și cel privat în scopul de a sprijini cooperarea și schimbul de informații la scară mai largă între un număr mai mare de sectoare. Rolul centrelor de schimb de informații și de analiză este deosebit de important în a crea încrederea necesară pentru realizarea schimbului de informații între sectorul privat și cel public. Au fost inițiate câteva prime demersuri în ceea ce privește anumite sectoare critice, cum ar fi sectorul aviației, prin crearea Centrului european pentru securitate cibernetică în sectorul aviației[35], și sectorul energiei, prin instituirea centrelor de schimb de informații și de analiză[36]. Comisia va contribui pe deplin la această abordare cu sprijinul ENISA, fiind necesară o accelerare în special în ceea ce privește sectoarele care furnizează servicii esențiale, astfel cum au fost identificate în Directiva NIS.

2.4 Reziliență prin reacția rapidă în caz de urgență

Atunci când are loc un atac cibernetic, o reacție rapidă și eficientă poate atenua impactul acestuia. De asemenea, o astfel de reacție poate demonstra că autoritățile publice nu sunt neputincioase în fața atacurilor cibernetice și poate contribui la crearea unui climat de încredere. În ceea ce privește propria reacție a instituțiilor UE, în primul rând, aspectele cibernetice ar trebui integrate în mecanismele UE existente de gestionare a crizelor: mecanismul integrat al UE pentru un răspuns politic la crize, coordonat de Președinția Consiliului[37], și sistemele generale de alertă rapidă ale UE[38]. Necesitatea de a răspunde la un

[33] COM(2017) 476.

[34] Securitatea cibernetică pe piața unică digitală europeană, grupul la nivel înalt de consilieri științifici, martie 2017. O problemă specifică se referă la secretele comerciale, pentru care comunicarea din iulie 2016 „Consolidarea sistemului de reziliență cibernetică al Europei" a remarcat reticența de a raporta furtul cibernetic de secrete comerciale și importanța canalelor de raportare de încredere care să asigure confidențialitatea.

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

[36] Acestea sunt organizații fără scop lucrativ, a căror activitate este desfășurată de membri, formate din entități private și publice care efectuează schimburi de informații privind amenințările cibernetice, riscurile, prevenirea, atenuarea și reacția. A se vedea, de exemplu, centrele europene de schimb de informații și de analiză în domeniul energiei (http://www.ee-isac.eu).

[37] Acesta permite coordonarea răspunsurilor la crizele majore intersectoriale la cel mai înalt nivel politic.

incident sau un atac cibernetic deosebit de grav ar putea constitui un motiv suficient pentru ca un stat membru să invoce clauza de solidaritate a UE[39].

O reacție rapidă și eficace se bazează, de asemenea, pe un mecanism rapid de schimb de informații între toți actorii importanți la nivel național și la nivelul UE, care necesită, la rândul său, claritate cu privire la rolurile și responsabilitățile care revin fiecăruia dintre aceștia. Comisia a consultat instituțiile și statele membre cu privire la un „plan de acțiune” pentru a asigura un proces eficace pentru un răspuns operațional la nivelul Uniunii și al statelor membre la un incident cibernetic la scară largă. **Planul de acțiune** prezentat în cadrul unei recomandări[40] din acest pachet explică modul în care securitatea cibernetică este integrată în mecanismele existente de gestionare a crizei la nivelul UE și stabilește obiectivele și modalitățile de cooperare între statele membre, precum și între statele membre și instituțiile, serviciile, agențiile și organismele UE relevante[41] atunci când răspund incidentelor și crizelor de securitate cibernetică de mare amploare. De asemenea, recomandarea solicită statelor membre și instituțiilor UE să instituie un cadru UE de răspuns la crizele de securitate cibernetică pentru a pune în aplicare planul de acțiune. Planul de acțiune va fi testat periodic în cadrul exercițiilor de gestionare a incidentelor cibernetice și a altor crize[42] și va fi actualizat în funcție de necesități.

Având în vedere că incidentele de securitate cibernetică ar putea avea un impact semnificativ asupra funcționării economiilor și asupra vieții cotidiene a cetățenilor, o opțiune ar fi examinarea posibilității de a lansa un **fond de răspuns la situații de urgență legate de securitatea cibernetică,** urmând exemplul altor astfel de mecanisme de gestionare a crizei din alte domenii de politică ale UE. Acesta ar permite statelor membre să solicite ajutor la nivelul UE pe perioada sau în urma unui incident major, cu condiția ca statul membru să fi instituit un sistem prudent de securitate cibernetică înainte de incident, care să includă punerea în aplicare pe deplin a Directivei NIS, gestionarea pertinentă a riscului și cadre de supraveghere la nivel național. Un astfel de fond, care completează mecanismele existente de gestionare a crizei la nivelul UE, ar putea utiliza capacitatea de răspuns rapid în vederea solidarității și ar finanța acțiunile de răspuns la situații de urgență specifice, cum ar fi înlocuirea echipamentelor compromise sau utilizarea instrumentelor de atenuare sau de răspuns, pe baza experiențelor naționale, după modelul mecanismului UE de protecție civilă.

2.5 O rețea de competențe în materie de securitate cibernetică împreună cu centrul european de competențe și de cercetare în materie de securitate cibernetică

Instrumentele tehnologice pentru securitatea cibernetică reprezintă avantaje strategice, precum și tehnologii esențiale pentru creșterea economică în viitor. Este în interesul strategic al UE să se asigure că Uniunea își menține și își dezvoltă capacitățile esențiale pentru a-și consolida economia digitală, societatea și democrația, pentru a proteja componentele hardware și programele informatice critice și pentru a furniza servicii esențiale în materie de securitate cibernetică.

---

[38] Acestea permit schimbul de informații și coordonarea la nivel intern în privința crizelor multisectoriale emergente sau a amenințărilor iminente ori previzibile care necesită o acțiune la nivelul UE.

[39] În temeiul articolului 222 din Tratatul privind funcționarea Uniunii Europene.

[40] C(2017) 6100.

[41] Inclusiv Europol, ENISA, Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE) și Centrul de analiză a informațiilor al UE (INTCEN).

[42] De exemplu, cele desfășurate de ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Parteneriatul public-privat privind securitatea cibernetică[43] creat în 2016 a fost un prim pas important, generând investiții de până la 1,8 miliarde EUR până în 2020. Cu toate acestea, amploarea investițiilor în curs în alte părți ale lumii[44] sugerează că UE trebuie să depună mai multe eforturi în ceea ce privește investițiile și să contracareze fragmentarea capacităților în cadrul UE.

UE are valoare adăugată pentru a furniza, având în vedere complexitatea tehnologiei în materie de securitate cibernetică, investițiile pe scară largă necesare, precum și nevoia de soluții care să funcționeze la nivelul întregii Uniuni. Pe baza activităților desfășurate de statele membre și a parteneriatului public-privat, următorul pas ar consta în consolidarea capacității UE în materie de securitate cibernetică prin intermediul unei **rețele de centre de competențe în materie de securitate cibernetică**[45], reunită în jurul unui **centru european de competențe și de cercetare în materie de securitate cibernetică**. Această rețea și centrul său ar stimula dezvoltarea și utilizarea tehnologiei în domeniul securității cibernetice și ar completa eforturile de consolidare a capacității în domeniu la nivelul UE și la nivel național. Comisia va lansa o evaluare a impactului pentru a examina opțiunile disponibile – inclusiv posibilitatea de a înființa o întreprindere comună – cu scopul de a institui această structură în 2018.

Ca un prim pas și pentru a sta la baza viitoarelor idei, Comisia va propune lansarea unei etape pilot în cadrul programului Orizont 2020 pentru a sprijini reunirea centrelor naționale în cadrul unei rețele în scopul de a crea o nouă dinamică în domeniul securității cibernetice și în dezvoltarea tehnologică. Comisia urmărește să propună o injecție pe termen scurt de fonduri în valoare de 50 de milioane EUR în acest scop. Activitatea va completa punerea în aplicare în curs a parteneriatului public-privat privind securitatea cibernetică.

Punerea în comun și modelarea eforturilor de cercetare ar reprezenta nucleul rețelei și obiectivul inițial al centrului. Pentru a sprijini dezvoltarea capacităților industriale, centrul ar putea acționa în calitate de administrator al proiectului în materie de capacitate, în măsură să gestioneze proiecte multinaționale. De asemenea, acest lucru ar da un nou impuls inovării și competitivității industriei UE pe scena globală în ceea ce privește dezvoltarea următoarei generații de tehnologii digitale, inclusiv inteligența artificială, informatica cuantică, tehnologia blockchain și identitățile digitale securizate, precum și în asigurarea accesului la date în masă pentru societățile cu sediul în UE, toate acestea fiind esențiale pentru securitatea cibernetică în viitor. Centrul se va baza, de asemenea, pe activitatea UE pentru a dezvolta infrastructură de calcul de înaltă performanță: aceasta este esențială pentru analiza unor cantități mari de date, criptarea și decriptarea rapidă a datelor, verificarea identităților, simularea atacurilor cibernetice și analiza materialelor video[46].

De asemenea, rețeaua de centre de competențe ar putea dispune de capacitatea de a sprijini industria prin testare și simulare pentru a susține certificarea în materie de securitate cibernetică descrisă în secțiunea 2.2. Implicarea rețelei în întreaga gamă de activități în domeniul securității cibernetice la nivelul UE ar asigura o permanentă actualizare a obiectivului acesteia în funcție de nevoi. Centrul ar avea drept obiectiv atingerea unor standarde ridicate de securitate cibernetică nu numai în cadrul sistemelor tehnologice și de securitate cibernetică, ci și în dezvoltarea de competențe de înaltă calitate pentru specialiști,

[43] C(2016) 4400 final.

[44] SUA va investi 19 miliarde USD în securitatea cibernetică numai în 2017, cu o creștere de 35 % în comparație cu 2016. Secretarul Oficiului de Presă al Casei Albe: „Fișă informativă: Planul național de acțiune în domeniul securității cibernetice”, 9 februarie 2016.

[45] Rețeaua ar urma să includă centrele de securitate cibernetică existente și viitoare înființate în statele membre, ale căror membri ar fi, în general, organizații și laboratoare publice de cercetare.

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

prin furnizarea de soluții și modele pentru eforturile naționale de extindere a competențelor digitale. În acest sens, centrul ar trebui, de asemenea, să consolideze capacitățile în domeniul securității cibernetice la nivelul UE și să valorifice sinergiile, în special cu ENISA, CERT-UE, Europol, posibilul viitor fond de răspuns la situații de urgență legate de securitatea cibernetică și echipele CSIRT naționale.

În activitatea desfășurată de rețeaua de competențe, o atenție deosebită trebuie acordată lipsei de capacitate europeană de a evalua **criptarea** produselor și a serviciilor utilizate de cetățeni, întreprinderi și administrații publice în cadrul pieței unice digitale. Un nivel ridicat de criptare reprezintă baza pentru sisteme de identificare digitală securizate, care au un rol-cheie în securitatea cibernetică eficace[47]; de asemenea, acesta menține în siguranță proprietatea intelectuală a oamenilor și permite protejarea drepturilor fundamentale, precum libertatea de exprimare și protecția datelor cu caracter personal, și asigură un mediu sigur pentru comerțul online[48].

Întrucât piețele securității cibernetice civile și de apărare împărtășesc provocări comune[49], iar tehnologiile cu dublă utilizare necesită o colaborare strânsă în domeniil critice, ar putea fi dezvoltată în continuare o a doua etapă a rețelei și a centrului său cu o dimensiune de apărare cibernetică, cu respectarea deplină a dispozițiilor tratatului referitoare la politica comună de securitate și apărare. La fel ca orientarea sa tehnologică, dimensiunea de apărare ar putea contribui la cooperarea între statele membre în domeniul apărării împotriva criminalității cibernetice, inclusiv prin schimbul de informații, cunoașterea situației, dobândirea de competențe și reacții coordonate, precum și sprijinirea dezvoltării de capacități comune de către statele membre. De asemenea, aceasta ar putea acționa ca o platformă, care le permite statelor membre să identifice prioritățile pentru apărarea UE împotriva criminalității cibernetice, să examineze soluții comune, să contribuie la elaborarea de strategii comune, să faciliteze desfășurarea cursurilor, exercițiilor și testărilor comune de apărare împotriva criminalității cibernetice la nivel european, precum și să sprijine activitățile privind clasificările și standardele în materie de apărare cibernetică, centrul având un rol consultativ și de sprijin. Pentru a desfășura activitățile menționate mai sus, centrul ar trebui să colaboreze îndeaproape și în deplină complementaritate cu Agenția Europeană de Apărare în domeniul apărării cibernetice, precum și cu ENISA în domeniul rezilienței cibernetice. Această dimensiune de apărare ar lua în considerare procesul lansat de Documentul de reflecție privind viitorul apărării europene.

Nivelul ridicat de reziliență necesar în domeniul apărării împotriva criminalității cibernetice necesită o orientare specifică a eforturilor în materie de cercetare și de tehnologie. Proiectele de apărare împotriva criminalității cibernetice sau tehnologiile dezvoltate de întreprinderi ar putea beneficia de finanțare din partea Fondului european de apărare europeană în ceea ce privește atât cercetarea, cât și etapa de dezvoltare[50]. Domenii specifice cum ar fi sistemele de criptare bazate pe tehnologiile cuantice, cunoașterea situației cibernetice, sistemele de control al accesului pe baza datelor biometrice, detectarea amenințărilor avansate persistente sau

---

[47] Comisia va lansa, în cadrul programului Orizont 2020, o nouă provocare a Premiilor Orizont, prin care se va acorda un premiu în valoare de 4 milioane EUR pentru cea mai bună soluție inovatoare în ceea ce privește metodele de autentificare online fără dificultăți.

[48] Securitatea cibernetică pe piața unică digitală europeană, grupul la nivel înalt de consilieri științifici, martie 2017.

[49] „Studiu privind sinergiile între piețele securității cibernetice civile și de apărare” (Optimity; SMART 2014-0059).

[50] În prezent, Programul de dezvoltare a industriei de apărare europene va acorda deja prioritate proiectelor de apărare împotriva criminalității cibernetice, iar apărarea împotriva criminalității cibernetice va fi una dintre temele din cadrul cererii de propuneri care va fi lansată în 2018.

extragerea de date ar putea fi deosebit de relevante în acest context. Înaltul Reprezentant, Agenția Europeană de Apărare și Comisia vor sprijini statele membre în identificarea domeniilor în care ar putea fi luate în considerare proiecte comune în materie de securitate cibernetică pentru finanțări din partea Fondului european de apărare.

2.6 Construirea unei baze de competențe cibernetice solide la nivelul UE

Există o puternică dimensiune educațională în ceea ce privește securitatea cibernetică. Securitatea cibernetică eficace se bazează în mare măsură pe competențele persoanelor vizate. Cu toate acestea, lipsa de specialiști având competențe în materie de securitate cibernetică care să lucreze în sectorul privat în Europa va fi, conform estimărilor, de 350 000 până în 2022[51]. Educația în materie de securitate cibernetică ar trebui dezvoltată la toate nivelurile, pornind de la formarea periodică a unui forțe de muncă din domeniul cibernetic, cursuri de formare suplimentare în materie de securitate cibernetică pentru toți specialiștii din domeniul TIC și noile programe specifice în materie de securitate cibernetică. Ar trebui stabilite centre de competențe academice solide pentru a răspunde solicitărilor de educație și formare într-un ritm mai accelerat, care ar putea să se bazeze pe orientare din partea Centrului european de competențe și de cercetare în materie de securitate cibernetică și a ENISA. Obiectivul urmărit este generalizarea unui proces de concepere a produselor și sistemelor TIC care integrează principii de securitate încă de la început. Educația în materie de securitate cibernetică nu ar trebui să fie limitată la specialiștii din domeniul informatic, ci ar trebui să fie inclusă în programele de studiu din alte domenii, cum ar fi ingineria, administrarea afacerilor sau dreptul, precum și în filierele educaționale sectoriale specifice. În final, cadrele didactice și elevii din învățământul primar și secundar ar trebui să fie informați cu privire la criminalitatea cibernetică și securitatea cibernetică atunci când dobândesc competențe digitale în școli.

De asemenea, UE, împreună cu statele membre, ar trebui să contribuie la această activitate pornind de la activitatea Coaliției pentru competențe și locuri de muncă în sectorul digital[52] și prin instituirea, de exemplu, a programelor de ucenicie în domeniul securității cibernetice pentru IMM-uri.

2.7 Promovarea conștientizării și a igienei cibernetice

Având în vedere faptul că aproximativ 95 % din incidente au loc ca urmare a unui „anumit tip de eroare umană – fie aceasta intenționată sau nu”[53], este implicat un factor uman important. Prin urmare, securitatea cibernetică este o responsabilitate colectivă. Aceasta înseamnă că trebuie să fie modificat comportamentul persoanelor, al întreprinderilor și al administrației publice pentru a garanta faptul că fiecare conștientizează amenințarea și este echipat cu instrumentele și competențele necesare pentru a detecta rapid atacurile și a se proteja în mod activ împotriva acestora. Oamenii trebuie să dezvolte obiceiuri de igienă cibernetică, iar întreprinderile și organizațiile trebuie să adopte programe în materie de securitate cibernetică adecvate și bazate pe risc și să le actualizeze periodic pentru a reflecta mediul de risc în continuă schimbare.

Pe lângă faptul că Directiva NIS stabilește responsabilitățile statelor membre de a efectua schimburi de informații privind atacurile cibernetice la nivelul UE, aceasta pune în aplicare

---

[51] Studiul global privind forța de muncă în domeniul securității informațiilor, 2017. Deficitul global este de 1,8 milioane EUR.

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

[53] IBM, „The Cybersecurity Intelligence Index” (Raport privind securitatea cibernetică) 2014, menționat în securitymagazine.com, 19 iunie 2014.

strategii naționale în domeniul securității cibernetice și cadre privind securitatea rețelelor și a sistemelor informatice bine stabilite. Administrațiile publice la nivelul UE și la nivel național ar trebui să joace un rol de lider în dezvoltarea acestor eforturi.

În primul rând, statele membre ar trebui să maximizeze disponibilitatea instrumentelor de securitate cibernetică pentru întreprinderi și persoane. În special, ar trebui depuse mai multe eforturi pentru a preveni și a atenua efectele criminalității cibernetice asupra utilizatorilor finali. Un exemplu îl constituie deja activitatea desfășurată de Europol prin campania „NoMoreRansom”[54], care se bazează pe o strânsă cooperare între autoritățile de aplicare a legii și întreprinderile din domeniul securității cibernetice pentru a sprijini utilizatorii să prevină infecțiile cu programe de șantaj digital să decripteze datele în cazul în care aceștia sunt victime ale unui atac cibernetic. Astfel de programe ar trebui să fie extinse la alte tipuri de programe rău-intenționate din alte domenii, iar UE ar trebui să creeze **un portal unic pentru a reuni toate aceste instrumente într-un ghișeu unic**, care să ofere consultanță utilizatorilor cu privire la prevenirea și detectarea programelor rău-intenționate și linkuri către mecanisme de raportare.

În al doilea rând, statele membre ar trebui să accelereze **utilizarea instrumentelor mai sigure din punct de vedere cibernetic în dezvoltarea guvernării electronice** și, de asemenea, să beneficieze pe deplin de rețeaua de competențe. Ar trebui promovată adoptarea unor mijloace securizate de identificare, pe baza cadrului UE de identificare electronică și de servicii de asigurare a încrederii pentru tranzacțiile electronice pe piața internă care a intrat în vigoare în 2016 și prevede un mediu de reglementare previzibil pentru a permite interacțiuni electronice sigure și fără întreruperi între întreprinderi, persoane și autorități publice[55]. În plus, instituțiile publice, în special cele care furnizează servicii esențiale, ar trebui să se asigure că personalul acestora este instruit în domenii legate de securitatea cibernetică.

În al treilea rând, statele membre ar trebui să considere conștientizarea securității cibernetice ca fiind o prioritate **în campaniile de conștientizare**, inclusiv cele care vizează școlile, universitățile, comunitatea de afaceri și organismele de cercetare. Activitățile desfășurate pe parcursul lunii dedicate securității cibernetice, care are loc în fiecare an în octombrie sub coordonarea ENISA, vor fi intensificate pentru a obține o rază de acțiune mai mare ca un efort comun de comunicare la nivelul UE și la nivel național. Creșterea gradului de conștientizare cu privire la **campaniile de dezinformare și știrile false** online pe platformele de comunicare socială, care vizează în mod specific subminarea proceselor democratice și a valorilor europene, este la fel de importantă. Deși responsabilitatea principală rămâne la nivel național – inclusiv pentru alegerile din cadrul Parlamentului European – punerea în comun a cunoștințelor și schimbul de experiență la nivel european s-au dovedit a fi un instrument cu valoare adăugată în furnizarea unui obiectiv de acțiune[56].

De asemenea, un rol important revine **sectorului industrial** în general, însă cu o atenție deosebită acordată furnizorilor și producătorilor de servicii digitale. Aceasta trebuie să sprijine utilizatorii (persoane, întreprinderi și administrații publice) cu instrumente care le

---

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

[55] Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (Regulamentul eIDAS), adoptat la 23 iulie 2014. De asemenea, Comisia Europeană oferă elemente constitutive și instrumente pentru interoperabilitatea identificării electronice și a semnăturii electronice (de exemplu, *Trusted Lists Browsers* - Instrumente de navigare pentru listele sigure) prin intermediul mecanismului „Interconectarea Europei”.

[56] Un exemplu în acest sens este grupul operativ East StratCom, instituit în 2015 de statele membre și Înaltul Reprezentant pentru a aborda campaniile de dezinformare în curs ale Rusiei. Echipa este implicată în dezvoltarea de produse și campanii de comunicare axate pe explicarea politicilor UE în regiunea Parteneriatului estic.

permit să își asume responsabilitatea pentru propriile acțiuni în mediul online, clarificând faptul că menținerea igienei cibernetice este o parte indispensabilă a ofertei pentru consumatori[57]. Pentru a detecta și a elimina vulnerabilitățile, industria ar trebui să depună eforturi pentru a dispune de procese interne care vizează investigarea, trierea și soluționarea vulnerabilităților, indiferent dacă sursa potențialei vulnerabilități provine din exteriorul sau interiorul întreprinderii în cauză.

Acțiuni-cheie

- punerea în aplicare pe deplin a Directivei privind securitatea rețelelor și a sistemelor informatice;
- adoptarea rapidă de Parlamentul European și Consiliu a regulamentului de stabilire a unui nou mandat pentru ENISA și a unui cadru european de certificare[58];
- o inițiativă comună a Comisiei/industriei pentru a defini principiul „obligației de diligență" în vederea reducerii vulnerabilităților produselor/programelor informatice și a promovării „securității din stadiul conceperii";
- punerea rapidă în aplicare a planului de acțiune pentru răspunsul în caz de incidente majore la nivel transfrontalier;
- lansarea unei evaluări a impactului pentru a studia posibilitatea prezentării de către Comisie în 2018 a unei propuneri privind instituirea unei rețele de centre de competențe în materie de securitate cibernetică și a unui centru european de competențe și de cercetare în materie de securitate cibernetică, pornind de la o etapă pilot imediată;
- sprijinirea statelor membre în identificarea domeniilor în care proiectele comune în materie de securitate cibernetică ar putea fi luate în considerare pentru a beneficia de sprijin din partea Fondului european de apărare;
- un ghișeu unic la nivelul UE pentru a sprijini victimele atacurilor cibernetice, prin furnizarea de informații privind ultimele amenințări și punerea în comun de sfaturi practice și instrumente de securitate cibernetică;
- măsuri luate de statele membre pentru a integra securitatea cibernetică în programele de dezvoltare a competențelor, guvernarea electronică și campaniile de informare;
- acțiuni întreprinse de societățile din domeniu pentru a intensifica formarea personalului propriu în aspecte legate de securitatea cibernetică și pentru a adopta o abordare de tip „securitate din stadiul conceperii" pentru produsele, serviciile și procesele lor.

3. ELABORAREA UNOR MĂSURI EFICACE DE DESCURAJARE A ATACURILOR CIBERNETICE LA NIVELUL UE

O descurajare eficace a atacurilor înseamnă instituirea unui cadru de măsuri care sunt atât credibile, cât și disuasive pentru potențialii infractori și atacatori din spațiul cibernetic. Atât timp cât autorii atacurilor cibernetice – atât statali, cât și nestatali – nu se tem decât de eșec, aceștia nu vor fi motivați să înceteze atacurile. Un răspuns mai eficace al autorităților de aplicare a legii, care se concentrează pe detectarea, identificarea și urmărirea penală a infractorilor cibernetici, este esențial pentru consolidarea unei descurajări eficace. La acesta se adaugă necesitatea ca UE să sprijine statele sale membre în dezvoltarea capacităților cu dublă utilizare în materie de securitate cibernetică. Nu vom începe să schimbăm situația privind atacurile cibernetice decât atunci când vom mări șansele de a prinde și a sancționa infractorii

[57] Unii producători sunt deja obișnuiți cu acest concept, deoarece unele acte legislative privind produsele (cum ar fi Directiva 2006/42/CE privind echipamentele tehnice) prevăd principii pentru „siguranța din stadiul conceperii".

[58] COM(2017) 477.

pentru comiterea acestora. Atacurile cibernetice ar trebui să fie rapid cercetate, iar autorii să fie aduși în fața justiției, sau ar trebui luate măsuri pentru a permite un răspuns politic sau diplomatic adecvat. În cazul unei crizei majore cu o importantă dimensiune internațională și de apărare, Înaltul Reprezentant ar putea prezenta Consiliului o serie de opțiuni pentru un răspuns adecvat.

Un pas către îmbunătățirea răspunsului în materie de drept penal la atacurile cibernetice a fost deja realizat odată cu adoptarea Directivei privind atacurile împotriva sistemelor informatice[59] în 2013. Aceasta stabilește norme minime privind definirea infracțiunilor și a sancțiunilor penale în domeniul atacurilor împotriva sistemelor informatice și prevede măsuri operaționale de îmbunătățire a cooperării între autorități. Directiva a condus la progrese semnificative în ceea ce privește incriminarea atacurilor cibernetice la un nivel comparabil în toate statele membre, ceea ce facilitează cooperarea transfrontalieră a autorităților de aplicare a legii care investighează aceste tipuri de infracțiuni. Cu toate acestea, există posibilități încă neexploatate pentru ca directiva să își atingă potențialul maxim în cazul în care statele membre ar pune în aplicare pe deplin toate dispozițiile acesteia[60]. Comisia va continua să ofere sprijin statelor membre în punerea în aplicare a directivei și, în prezent, nu consideră necesar să propună modificări la aceasta.

3.1 Identificarea actorilor răuvoitori

Pentru a ne spori șansele de a aduce făptașii în fața justiției, trebuie să ne îmbunătățim capacitatea de a-i identifica pe cei responsabili de atacurile cibernetice. Găsirea de informații utile pentru investigațiile privind criminalitatea cibernetică, în special sub formă de urme digitale, reprezintă o provocare majoră pentru autoritățile de aplicare a legii. Prin urmare, este necesar să ne sporim capacitatea tehnologică pentru a investiga în mod eficace, inclusiv prin consolidarea unității de combatere a criminalității cibernetice a Europol, formată din experți în securitate cibernetică. Europol a devenit un actor cheie în sprijinirea investigațiilor multijurisdicționale ale statelor membre. Acesta ar trebui să devină un centru de expertiză pentru aplicarea legii de către statele membre în ceea ce privește anchetele realizate în spațiul online și criminalistica cibernetică.

Practica larg răspândită de a plasa mai mulți utilizatori – uneori mii – în spatele unei singure adrese IP îngreunează din punct de vedere tehnic investigarea comportamentului rău intenționat în spațiul online. De asemenea, aceasta face necesară, de exemplu pentru infracțiunile grave precum abuzul sexual asupra copiilor, investigarea unui număr mare de utilizatori cu scopul de a identifica un singur actor răuvoitor. Prin urmare, UE va încuraja adoptarea noului protocol (IPv6), întrucât acesta permite alocarea unui singur utilizator pe adresă IP, aducând astfel beneficii clare pentru autoritățile de aplicare a legii și anchetele în materie de securitate cibernetică. Ca un prim pas pentru încurajarea adoptării acestuia, Comisia va integra obligația de a trece la protocolul IPv6 în politicile acesteia, inclusiv cerințele privind finanțarea achizițiilor publice, a proiectelor și a cercetării, precum și sprijinirea materialelor necesare pentru formare. În plus, statele membre ar trebui să ia în considerare acorduri voluntare cu furnizorii de servicii de internet pentru a stimula adoptarea protocolului IPv6.

[59] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice.

[60] COM(2017)474.

Belgia este pe primul loc în lume[61] în ceea ce privește rata adoptării IPv6, datorită, de asemenea, cooperării dintre sectorul public și cel privat: părțile interesate relevante au luat în considerare limitarea utilizării unei adrese IP la maximum 16 utilizatori, ca parte a unei măsuri de autoreglementare voluntară, care a stimulat tranziția către IPv6[62].

La un nivel general, responsabilizarea în spațiul online ar trebui să fie promovată în continuare. Aceasta înseamnă promovarea unor măsuri pentru a preveni utilizarea abuzivă a numelor de domenii pentru distribuția de mesaje nesolicitate sau atacurile de tip phishing. În acest scop, Comisia va depune eforturi pentru a îmbunătăți funcționarea, precum și disponibilitatea și exactitatea informațiilor în sistemele WHOIS[63] de nume de domenii și IP în concordanță cu eforturile Corporației pentru alocarea de nume și numere de domenii internet - *Internet Corporation for Assigned Names and Numbers*[64].

3.2 Intensificarea răspunsului autorităților de aplicare a legii

Cercetarea și **urmărirea penală** eficace a infracțiunilor cibernetice reprezintă un mijloc important de descurajare a atacurilor cibernetice. Cu toate acestea, cadrul procedural actual trebuie să fie mai bine adaptat la era internetului[65]. Atacurile cibernetice pot depăși procedurile noastre și conduc la crearea unor nevoi speciale de cooperare rapidă la nivel transfrontalier. În acest scop, astfel cum s-a anunțat în Agenda europeană privind securitatea, la începutul anului 2018 Comisia va prezenta propuneri pentru a **facilita accesul transfrontalier la probele electronice**. În paralel, Comisia pune în aplicare măsuri practice menite să îmbunătățească accesul transfrontalier la probele electronice pentru anchetele penale, inclusiv finanțarea pentru formarea privind cooperarea transfrontalieră, dezvoltarea unei platforme electronice pentru schimbul de informații în cadrul UE și standardizarea formularelor de cooperare judiciară utilizate între statele membre.

Un alt obstacol în calea urmăririi penale eficace este reprezentat de diferitele proceduri criminalistice pentru strângerea probelor electronice în cadrul anchetelor privind criminalitatea cibernetică din statele membre. Acesta ar putea fi atenuat prin acțiuni în vederea stabilirii unor standarde comune în materie de criminalistică. În plus, pentru a sprijini trasabilitatea și atribuirea, capacitățile criminalistice trebuie să fie consolidate. Un pas ar fi dezvoltarea în continuare a capacității criminalistice în cadrul Europol, adaptând resursele bugetare și umane existente în cadrul Centrului european de combatere a criminalității cibernetice al Europol pentru a satisface nevoia sporită de sprijin operațional în cadrul anchetelor transfrontaliere privind criminalitatea cibernetică. Un alt pas ar fi reflectarea orientării tehnologice stabilite mai sus pentru procesul de criptare, prin analizarea modului în care utilizarea abuzivă a criptării de către infractori creează importante provocări în lupta împotriva formelor grave de criminalitate, inclusiv împotriva terorismului și criminalității

---

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

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

63 Un protocol de interogare și răspuns care este utilizat la scară largă pentru interogarea bazelor de date care conțin utilizatorii înregistrați sau deținătorii unei resurse a internetului.

64 Corporația pentru alocarea de nume și numere de domenii internet - *Internet Corporation for Assigned Names and Numbers* (ICANN) este o organizație fără scop lucrativ, responsabilă de coordonarea procedurilor de întreținere a mai multor baze de date referitoare la spațiile de nume de pe internet.

65 Pentru a oferi doar un exemplu, serverul central (virtual) de comandă și control al botnet-ului Avalanche a transferat serverele fizice și domeniile o dată la fiecare cinci minute.

cibernetice. Comisia va prezenta rezultatele reflecțiilor actuale privind **rolul criptării în anchetele penale**[66] până în octombrie 2017[67].

Având în vedere caracterul „fără frontiere” al internetului, cadrul pentru cooperarea internațională prevăzut de **Convenția de la Budapesta privind criminalitatea cibernetică**[68] a Consiliului Europei oferă posibilitatea în cadrul unui grup divers de țări de a utiliza un standard juridic optim pentru diferitele legislații naționale care abordează criminalitatea cibernetică. În prezent, se ia în considerare posibilitatea de a adăuga un protocol la convenție[69], ceea ce ar putea oferi, de asemenea, o oportunitate utilă de a aborda problema accesului transfrontalier la probele electronice în contextul internațional. În locul creării de noi instrumente juridice internaționale pentru aspectele legate de criminalitatea cibernetică, UE solicită tuturor țărilor să elaboreze legislații naționale corespunzătoare și să continue cooperarea în cadrul internațional existent.

Disponibilitatea tot mai mare a instrumentelor de asigurare a anonimatului facilitează ascunderea infractorilor. „**Darknet**”[70] (internetul întunecat) a deschis noi căi pentru infractori, prin care aceștia pot avea acces la materiale conținând abuzuri sexuale asupra copiilor, droguri sau de arme de foc, adesea cu un risc scăzut de a fi descoperiți[71]. În prezent, acesta este, de asemenea, o sursă esențială de instrumente utilizate în criminalitatea cibernetică, cum ar fi instrumentele de tip malware și de piraterie. Comisia, împreună cu părțile interesate relevante, va analiza abordările naționale în scopul de a identifica noi soluții. Europol ar trebui să faciliteze și să sprijine investigațiile privind darknet-ul, să evalueze amenințările și să contribuie la stabilirea competenței și la prioritizarea cazurilor cu risc crescut, iar UE poate îndeplini un rol major în coordonarea acțiunii internaționale[72].

Un domeniu în creștere al activității de criminalitate cibernetică este utilizarea frauduloasă a detaliilor cărții de credit sau a altor mijloace electronice de plată. Elementele de plată obținute prin atacurile cibernetice asupra comercianților cu amănuntul din spațiul online sau asupra altor întreprinderi legitime sunt comercializate ulterior online și pot fi utilizate de infractori pentru a comite fraude[73]. Comisia prezintă o propunere care vizează sporirea acțiunilor de descurajare prin intermediul unei **directive privind combaterea fraudei și a falsificării altor**

---

66 Președinția Consiliului, „Rezultatele reuniunii Consiliului Justiție și Afaceri Interne din 8 și 9 decembrie 2016”, nr. 15391/16.

67 Al optulea raport referitor la progresele înregistrate pentru realizarea unei uniuni a securității efective și reale din 29 iunie 2017, COM(2017) 354 final.

68 Convenția este primul tratat internațional privind infracțiunile săvârșite prin intermediul internetului și al altor rețele informatice, vizând în special încălcările drepturilor de autor, frauda informatică, pornografia infantilă și încălcările securității rețelei. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 În 2017, 55 de guverne au ratificat sau au aderat la Convenția Consiliului Europei privind criminalitatea cibernetică.

69 Mandat de pregătire a unui proiect al celui de al doilea protocol adițional la Convenția de la Budapesta privind criminalitatea cibernetică, T-CY (2017)3.

70 Darknet-ul constă în conținut din rețele suprapuse care utilizează internetul, dar necesită software specific, anumite configurații sau autorizație de acces. Darknet-ul reprezintă o mică parte a webului invizibil, o porțiune din web care nu este indexată de motoarele de căutare.

71 O excepție notabilă o constituie închiderea recentă a două dintre cele mai mari piețe de bunuri ilegale de pe dark web, AlphaBay și Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Europol îndeplinește deja un rol important în acest domeniu. Pentru un exemplu recent, a se vedea: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

73 Câștigurile realizate în urma fraudelor reprezintă o sursă importantă de venituri pentru criminalitatea organizată și, prin urmare, un factor favorizant pentru alte activități infracționale precum terorismul, traficul de droguri și traficul de ființe umane.

modalități de plată decât numerarul[74]. Aceasta urmărește să actualizeze normele existente în domeniu și să consolideze capacitatea autorităților de aplicare a legii de a combate această formă de infracțiune.

Capacitățile de investigare a criminalității cibernetice ale autorităților de aplicare a legii din statele membre trebuie, de asemenea, să fie îmbunătățite, la fel ca înțelegerea infracțiunilor cibernetice și a opțiunilor de investigare de către procurori și sistemul judiciar. Eurojust și Europol contribuie la acest obiectiv și la o mai bună coordonare, în strânsă cooperare cu grupurile consultative specializate din cadrul Centrului de combatere a criminalității informatice al Europol și cu rețelele de șefi ai unităților de combatere a criminalității cibernetice și de procurori specializați în criminalitatea cibernetică. Comisia va aloca un fond de 10,5 milioane EUR pentru combaterea criminalității cibernetice, în special în cadrul programului **Fondul pentru securitate internă - Poliție**. Formarea profesională este un element important și o serie de materiale utile au fost elaborate de Grupul european de formare și educație în materie de combatere a criminalității informatice. Acestea ar trebui utilizate la scară largă de către specialiștii responsabili de aplicarea legii, cu sprijinul Agenției Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL).

3.3 Cooperarea dintre sectorul public și cel privat împotriva criminalității cibernetice

Eficacitatea mecanismelor tradiționale de aplicare a legii este pusă sub semnul întrebării de caracteristicile mediului digital, care este format în cea mai mare parte din infrastructură privată și numeroși actori diferiți din diverse jurisdicții. Prin urmare, cooperarea cu sectorul privat, inclusiv industria și societatea civilă, este esențială pentru autoritățile publice în scopul de a lupta eficace împotriva criminalității. În acest context, sectorul financiar este, de asemenea, esențial, iar cooperarea ar trebui intensificată. De exemplu, rolul unităților de informații financiare[75] în contextul criminalității cibernetice ar trebui să fie consolidat.

Unele state membre au luat deja măsuri esențiale. În Țările de Jos, instituțiile financiare și autoritățile de aplicare a legii colaborează pentru a combate frauda în mediul online și criminalitatea cibernetică în cadrul grupului operativ privind criminalitatea electronică. Centrul de competențe pentru combaterea criminalității cibernetice din Germania oferă membrilor săi platforma operațională pentru a efectua schimburi de informații, în strânsă colaborare cu Biroul Federal al Poliției germane, și pentru a elabora măsuri menite să asigure protecție împotriva criminalității cibernetice. 16 state membre[76] au înființat centre de excelență pentru combaterea criminalității cibernetice în scopul de a facilita cooperarea între autoritățile de aplicare a legii, mediul academic și partenerii privați în vederea elaborării și a schimbului de cele mai bune practici, a formării profesionale și a consolidării capacităților. Comisia sprijină stabilirea de parteneriate public-privat și de mecanisme de cooperare prin intermediul unor proiecte dedicate, cum ar fi Centrul cibernetic de combatere a fraudei online și Rețeaua de experți[77], prin care este pus în aplicare modelul și standardul de

[74] COM(2017) 489.

[75] Unitățile de informații financiare servesc drept centre naționale de primire și de analiză a rapoartelor privind tranzacțiile suspecte și a altor informații relevante privind cazurile de spălare a banilor, infracțiunile principale asociate și finanțarea terorismului, precum și de comunicare a rezultatelor obținute în urma analizei.

[76] Austria, Belgia, Bulgaria, Cipru, Republica Cehă, Estonia, Franța, Germania, Grecia, Irlanda, Lituania, Polonia, România, Slovenia, Spania și Regatul Unit.

[77] Inițiativa UE-OF2CEN urmărește realizarea unui schimbul sistematic la nivel comunitar de informații legate de frauda online între bănci și serviciile de aplicare a legii în scopul de a preveni efectuarea unor plăți către autorii fraudelor și persoanele care realizează transferuri de bani obținuți ilegal („money mules") și de a investiga și urmări penal autorii implicați. Aceasta este cofinanțată de UE (Programul Fondul pentru securitate internă - Poliție).

realizare a schimbului de informații pentru a analiza și a atenua riscurile de infracțiuni electronice și de fraude online.

În contextul criminalității cibernetice, întreprinderile private trebuie să fie capabile să realizeze schimburi de informații privind incidentele concrete cu autoritățile de aplicare a legii – inclusiv date cu caracter personal – cu respectarea deplină a normelor de protecție a datelor. Reforma UE în materie de protecție a datelor, care va intra în vigoare în mai 2018, prevede un set comun de norme cuprinzând condițiile în care autoritățile de aplicare a legii și entitățile private pot coopera. Comisia Europeană va colabora cu Comitetul european pentru protecția datelor și cu părțile interesate relevante pentru a identifica cele mai bune practici în acest domeniu și, după caz, pentru a furniza orientări.

3.4 Intensificarea răspunsului politic

Cadrul pentru un răspuns diplomatic comun al UE la activitățile cibernetice ostile[78] adoptat recent („setul de instrumente pentru diplomație în domeniul cibernetic") stabilește măsurile din cadrul politicii externe și de securitate comune, inclusiv măsuri restrictive care pot fi utilizate pentru a consolida răspunsul UE la activitățile care îi prejudiciază interesele politice, economice și de securitate. Cadrul constituie un pas important în dezvoltarea capacităților de semnalizare și de reacție la nivelul UE și al statelor membre. Acesta va spori capacitatea noastră de a atribui activitățile cibernetice ostile, cu scopul de a influența comportamentul potențialilor agresori, luând în considerare în același timp necesitatea de a se asigura răspunsuri proporționale. Atribuirea unei activități cibernetice ostile unui actor statal sau nestatal rămâne o decizie politică suverană pe baza informațiilor provenite din toate sursele. Activități de punere în aplicare a cadrului sunt, în prezent, în curs de desfășurare cu statele membre și, de asemenea, ar trebui continuate în strânsă coordonare cu planul de acțiune pentru a răspunde incidentelor cibernetice de mare amploare[79]. Procesul de cunoaștere a situației necesar pentru utilizarea măsurilor prevăzute în cadrul menționat ar trebui să fie corelat, analizat și diseminat de INTCEN[80], în strânsă colaborare cu statele membre și cu instituțiile UE.

3.5 Consolidarea descurajării în domeniul securității cibernetice prin intermediul capacității de apărare a statelor membre

Statele membre sunt deja implicate în dezvoltarea capacităților de apărare cibernetică. În plus, având în vedere estomparea delimitărilor dintre apărarea cibernetică și securitatea cibernetică și dubla utilizare a unor instrumente și tehnologii cibernetice, precum și diferențele considerabile între abordările statelor membre, UE se află în poziția potrivită pentru a contribui la promovarea sinergiilor între eforturile militare și cele civile[81].

Statele membre care dispun de capacități mai avansate în materie de securitate cibernetică și doresc să le pună în comun ar putea lua în considerare, cu sprijin din partea Înaltului Reprezentant, al Comisiei și al Agenției Europene de Apărare, includerea apărării împotriva criminalității cibernetice într-un cadru de „cooperare structurată permanentă" (PESCO). Acest lucru ar putea fi sprijinit de activitățile menționate mai sus pentru a încuraja capacitățile industriale ale UE și autonomia strategică. De asemenea, UE poate promova

[78] http://www.consilium.europa.eu/ro/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.
[79] C(2017) 6100.
[80] JOIN(2016) 018 final.
[81] În concepția UE, spațiul cibernetic este un spațiu de desfășurare a operațiunilor, la fel ca spațiul terestru, aerian și maritim. Eforturile în materie de apărare cibernetică includ, de asemenea, protecția și reziliența activelor spațiale și ale infrastructurilor de la sol aferente.

interoperabilitatea, inclusiv prin facilitarea dezvoltării capacităților, coordonarea formării profesionale și a educației, precum și eforturile de standardizare a dublei utilizări.

În plus, cadrul comun ar trebui valorificat pe deplin pentru a răspunde amenințărilor hibride care implică adesea atacuri cibernetice, în special prin intermediul celulei de fuziune a UE împotriva amenințărilor hibride și al centrului european pentru contracararea amenințărilor hibride din Helsinki, a cărui misiune este de a încuraja dialogul strategic și de a desfășura activități de cercetare și de analiză.

UE va plasa un accent reînnoit pe cadrul de politică al UE în domeniul apărării cibernetice din 2014[82], ca instrument pentru o asigura mai bună integrare a securității și apărării cibernetice în politica de securitate și de apărare comună (PSAC). Reziliența cibernetică a misiunilor și operațiunilor PSAC este esențială: vor fi elaborate proceduri standardizate și capacități tehnice care ar putea sprijini misiunile și operațiunile civile și militare desfășurate, precum și structurile lor respective privind capacitățile de planificare și conducere și furnizorii serviciilor de tehnologia informațiilor ai SEAE. Pentru a spori cooperarea între statele membre și pentru a orienta mai bine eforturile UE în domeniu, Agenția Europeană de Apărare și SEAE, în cooperare cu serviciile Comisiei, va facilita implicarea comună la nivel strategic a factorilor de decizie politică în materie de apărare cibernetică din statele membre. De asemenea, UE va sprijini elaborarea unor soluții de securitate cibernetică la nivel european ca parte a eforturilor sale de sprijinire a unei baze industriale și tehnologice de apărare europeană. Aceasta include, de asemenea, promovarea centrelor regionale de excelență în domeniul securității și apărării cibernetice.

Serviciile Comisiei, în strânsă cooperare cu SEAE, statele membre și alte organisme relevante ale UE, vor institui până la 2018 **o platformă de educație și formare în domeniul apărării cibernetice** pentru a aborda lacunele actuale în materie de competențe în domeniul apărării cibernetice. Aceasta va veni în completarea activităților în domeniu desfășurate de Agenția Europeană de Apărare, contribuind la abordarea actualelor lacune în materie de competențe în domeniul securității cibernetice și al apărării cibernetice.

Acțiuni-cheie

- o inițiativă a Comisiei pentru accesul transfrontalier la probele electronice (la începutul anului 2018);
- adoptarea rapidă de către Parlamentul European și Consiliu a propunerii de directivă privind combaterea fraudei și a falsificării altor mijloace de plată decât numerarul;
- introducerea unor cerințe privind protocolul IPv6 în ceea ce privește finanțarea de către UE a achizițiilor publice, a cercetării și a proiectelor; acordurile voluntare între statele membre și furnizorii de servicii de internet pentru a mări gradul de adoptare a protocolului IPv6;
- un accent reînnoit/extins în cadrul Europol în ceea ce privește criminalistica cibernetică și monitorizarea darknet-ului;
- punerea în aplicare a cadrului pentru un răspuns diplomatic comun al UE la activitățile cibernetice ostile;
- intensificarea sprijinului financiar pentru proiectele naționale și transnaționale care urmăresc îmbunătățirea justiției penale în spațiul cibernetic;
- o platformă educațională legată de securitatea cibernetică pentru a aborda lacunele actuale în materie de competențe în domeniul securității cibernetice și al apărării cibernetice în 2018.

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

4. CONSOLIDAREA COOPERĂRII LA NIVEL INTERNAȚIONAL ÎN DOMENIUL SECURITĂȚII CIBERNETICE

Ghidată de valorile fundamentale ale UE și de drepturile fundamentale, cum ar fi libertatea de exprimare și dreptul la viață privată și la protecția datelor cu caracter personal, precum și de promovarea unui spațiu cibernetic deschis, liber și sigur, politica internațională a UE în materie de securitate cibernetică este destinată să răspundă provocării aflate într-o evoluție continuă de a promova stabilitatea cibernetică la nivel mondial, precum și de a contribui la autonomia strategică a Europei în spațiul cibernetic.

4.1 Securitatea cibernetică în cadrul relațiilor externe

Dovezile sugerează că persoane din întreaga lume identifică atacurile cibernetice lansate din alte țări ca fiind printre principalele amenințări la adresa securității naționale[83]. Având în vedere natura globală a amenințării, crearea și menținerea unor alianțe și parteneriate solide cu țările terțe sunt fundamentale pentru prevenirea și descurajarea atacurilor cibernetice – care sunt tot mai importante pentru stabilitatea și securitatea internațională. UE va acorda prioritate instituirii unui cadru strategic pentru prevenirea conflictelor și asigurarea stabilității în spațiul cibernetic în cadrul angajamentelor sale bilaterale, regionale, multipartite și multilaterale.

UE promovează cu fermitate poziția conform căreia dreptul internațional, în special Carta Organizației Națiunilor Unite, se aplică spațiului cibernetic. Ca o completare la dispozițiile obligatorii de drept internațional, UE sprijină normele, reglementările și principiile voluntare, fără caracter obligatoriu, privind comportamentul responsabil al statului, care au fost enunțate de Grupul de experți guvernamentali al ONU[84]; de asemenea, aceasta încurajează dezvoltarea și punerea în aplicare a unor măsuri de consolidare a încrederii la nivel regional, atât în cadrul Organizației pentru Securitate și Cooperare din Europa, cât și în alte regiuni.

La nivel bilateral, dialogurile privind securitatea cibernetică[85] vor fi dezvoltate în continuare și completate de eforturile de a facilita cooperarea cu țările terțe pentru a consolida principiile diligenței și responsabilității statului în spațiul cibernetic. UE va acorda prioritate aspectelor ce țin de securitatea internațională în spațiul cibernetic în angajamentele sale internaționale, asigurând, în același timp, că securitatea cibernetică nu va deveni un pretext pentru protecția pieței și limitarea drepturilor și libertăților fundamentale, inclusiv a libertății de exprimare și a accesului la informații. O abordare cuprinzătoare a securității cibernetice necesită respectarea drepturilor omului, iar UE va continua să susțină valorile sale fundamentale la nivel global pe baza orientărilor UE în domeniul drepturilor omului privind libertatea în mediul online[86]. În această privință, UE subliniază importanța implicării tuturor părților interesate în guvernanța internetului.

De asemenea, Comisia a prezentat o propunere[87] de modernizare a controalelor exporturilor UE, inclusiv introducerea unor controale asupra exporturilor de tehnologii de supraveghere cibernetică critice care ar putea conduce la încălcări ale drepturilor omului sau care ar putea fi utilizate în mod abuziv împotriva securității proprii a UE, și își va intensifica dialogurile cu

---

83 Studiul global privind atitudinile, primăvara anului 2017, Centrul de Cercetare Pew.

84 A/68/98 și A/70/174.

85 În septembrie 2017, UE a purtat dialoguri privind securitatea cibernetică cu SUA, China, Japonia, Republica Coreea și India.

86 Orientările UE în domeniul drepturilor omului privind libertatea de exprimare în mediul online și offline.

87 COM(2016) 616.

țările terțe pentru a promova convergența la nivel mondial și comportamentul responsabil în acest domeniu.

4.2 Consolidarea capacității în domeniul securității cibernetice

Stabilitatea cibernetică globală se bazează pe capacitatea națională și locală a tuturor țărilor de a preveni și a reacționa la incidentele cibernetice și de a ancheta și a urmări în instanță cazurile de criminalitate cibernetică. Sprijinirea eforturilor de a construi reziliența națională în țările terțe va crește nivelul securității cibernetice la nivel global, cu consecințe pozitive pentru UE. Combaterea amenințărilor cibernetice care evoluează rapid ar sugera necesitatea unor eforturi de dezvoltare a formării, a politicii și a legislației, precum și a unei funcționări eficiente a centrelor de răspuns la incidente de securitate cibernetică și a unităților de combatere a criminalității cibernetice în toate țările la nivel global.

Începând cu 2013, UE a îndeplinit un rol principal în consolidarea capacităților internaționale în domeniul securității cibernetice și a corelat în mod sistematic aceste eforturi cu activitățile sale de cooperare pentru dezvoltare. UE va continua să promoveze un model de consolidare a capacității bazate pe drepturi, în conformitate cu abordarea Digital4Development[88]. Prioritățile pentru consolidarea capacităților vor fi reprezentate de vecinătatea UE și de țările în curs de dezvoltare care înregistrează o conectivitate în creștere rapidă și o dezvoltare rapidă a amenințărilor. Eforturile UE vor veni în completarea agendei de dezvoltare a UE, având în vedere Agenda 2030 pentru dezvoltare durabilă și eforturile globale pentru consolidarea capacității instituționale.

În scopul de a îmbunătăți capacitatea UE de a mobiliza expertiza sa colectivă pentru a sprijini consolidarea capacităților, ar trebui să fie instituită o rețea de consolidare a capacității cibernetice a UE, care să reunească SEAE, autoritățile din domeniul cibernetic ale statelor membre, agențiile UE, serviciile Comisiei, mediul academic și societatea civilă. Orientări privind consolidarea capacității cibernetice a UE vor fi elaborate în scopul de a contribui la o mai bună orientare politică și prioritizare a eforturilor depuse de UE în asistarea țărilor terțe.

De asemenea, UE va colabora cu alte părți interesate din acest domeniu pentru a evita suprapunerea eforturilor și a facilita o consolidare mai specifică a capacităților în diferite regiuni.

4.3 Cooperarea între UE și NATO

Pe baza progreselor semnificative deja înregistrate, UE va aprofunda cooperarea dintre UE și NATO privind securitatea cibernetică, amenințările hibride și apărarea, astfel cum se prevede în declarația comună din 8 iulie 2016[89]. Prioritățile includ promovarea interoperabilității prin cerințe și standarde coerente în materie de apărare cibernetică, consolidarea cooperării în materie de instruire și exerciții, armonizarea cerințelor privind instruirea.

De asemenea, UE și NATO vor încuraja cooperarea în materie de cercetare și inovare în domeniul apărării cibernetice și se vor baza pe actualul acord tehnic privind schimbul de informații legate de securitatea cibernetică între organismele lor respective din domeniul securității cibernetice[90]. Eforturile comune recente în ceea ce privește combaterea amenințărilor hibride, în special cooperarea între celula de fuziune a UE împotriva amenințărilor hibride și departamentul de analiză a amenințărilor hibride al NATO, ar trebui

[88] Documentul de lucru al serviciilor Comisiei SWD (2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] Capacitatea de răspuns la incidente informatice a CERT-UE și NATO (NCIRC).

să fie exploatate în continuare în vederea consolidării rezilienței și a răspunsului la crizele cibernetice. Continuarea cooperării între UE și NATO va fi încurajată prin exerciții de apărare cibernetică, cu implicarea SEAE și a altor entități ale UE și omologi NATO relevanți, inclusiv Centrul de excelență NATO pentru cooperare în domeniul apărării cibernetice de la Tallinn. Pentru prima dată, NATO și UE vor efectua exerciții coordonate și în paralel ca răspuns la un scenariu hibrid, în cadrul cărora rolul de lider va fi asumat de NATO în 2017 și, în mod similar, de UE în 2018. Următorul raport privind cooperarea între UE și NATO, care urmează să fie prezentat consiliilor lor respective în decembrie 2017, va oferi oportunitatea de a lua în considerare posibilitățile de a extinde și mai mult cooperarea, în special prin asigurarea unor mijloace de comunicare comune, sigure și solide între toate instituțiile și organismele relevante implicate, inclusiv ENISA.

Acțiuni-cheie

- consolidarea cadrului strategic pentru prevenirea conflictelor și asigurarea stabilității în spațiul cibernetic;
- instituirea unei noi rețele de consolidare a capacității pentru a sprijini capacitatea țărilor terțe de abordare a amenințărilor cibernetice, precum și elaborarea de orientări UE privind consolidarea capacității în domeniul securității cibernetice pentru o mai bună prioritizare a eforturilor UE;
- continuarea cooperării între UE și NATO, inclusiv participarea la exerciții coordonate și în paralel, precum și creșterea interoperabilității standardelor în materie de securitate cibernetică.

5. CONCLUZIE

Pregătirea UE în domeniul securității cibernetice este esențială atât pentru piața unică digitală, cât și pentru o uniune a securității și apărării. Consolidarea securității cibernetice europene și combaterea amenințărilor la adresa atât a obiectivelor civile, cât și a celor militare sunt esențiale.

Viitoarea reuniune la nivel înalt privind spațiul digital organizată de Președinția estoniană la vineri, 29 septembrie 2017 oferă o oportunitate de a demonstra voința comună de a poziționa securitatea cibernetică în centrul UE ca societate digitală. Ca parte a acestui angajament comun, Comisia invită statele membre să își asume angajamente cu privire la modul în care acestea intenționează să acționeze în domeniile în care dețin responsabilitatea principală. Aceasta ar trebui să includă consolidarea securității cibernetice prin:

- asigurarea punerii în aplicare depline și eficace a Directivei NIS până la 9 mai 2018, precum și a resurselor necesare pentru autoritățile publice responsabile de securitatea cibernetică în scopul de a-și îndeplini efectiv sarcinile;
- aplicarea acelorași norme pentru administrațiile publice, având în vedere rolul pe care acestea îl îndeplinesc în societate și în economie în ansamblu;
- furnizarea de formare profesională în domeniul securității cibernetice în cadrul administrației publice;
- prioritizarea conștientizării securității cibernetice în campaniile de informare și includerea securității cibernetice în cadrul programei de formare academică și profesională;
- utilizarea inițiativelor de „cooperare structurată permanentă” (PESCO) și Fondul european de apărare pentru a sprijini dezvoltarea de proiecte în domeniul apărării împotriva criminalității cibernetice.

Prezenta comunicare comună a stabilit amploarea provocării și gama de măsuri pe care UE le poate adopta. Avem nevoie de o Europă rezilientă, care își poate proteja cetățenii în mod eficace prin anticiparea posibilelor incidente de securitate cibernetică, prin instituirea unei protecții puternice în structurile sale și în comportamentul său, prin refacerea rapidă în urma oricărui atac cibernetic și prin descurajarea celor responsabili de astfel de atacuri. Prezenta comunicare propune măsuri specifice care vor consolida în continuare structurile și capacitățile UE în materie de securitate cibernetică într-un mod coordonat, cu deplina cooperare a statelor membre și a diferitelor structuri vizate ale UE și respectând competențele și responsabilitățile acestora. Punerea sa în aplicare va demonstra în mod clar că UE și statele sale membre vor coopera pentru a crea un standard în materie de securitate cibernetică proporțional cu provocările tot mai mari cu care se confruntă Europa în prezent.