COMISIA
EUROPEANĂ

Bruxelles, 5.7.2016
COM(2016) 410 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Consolidarea sistemului de reziliență cibernetică al Europei

și încurajarea unui sector al securității cibernetice competitiv și inovator

1. INTRODUCERE/CONTEXT

Numărul incidentelor de securitate cibernetică cauzează, zilnic, pagube economice considerabile atât pentru întreprinderile europene, cât și pentru economie în general. Astfel de incidente subminează încrederea cetățenilor și a întreprinderilor în societatea digitală. Furtul de secrete comerciale, de informații comerciale și de date cu caracter personal, perturbarea serviciilor, inclusiv a celor esențiale, precum și a infrastructurilor, conduc la pierderi economice de ordinul a sute de miliarde de euro în fiecare an[1]. Acestea pot avea, de asemenea, consecințe asupra drepturilor fundamentale ale cetățenilor și asupra societății, în general.

Strategia de securitate cibernetică a Uniunii Europene din 2013[2] („Strategia UE de securitate cibernetică") și principalul său obiectiv – Directiva privind securitatea rețelelor și a informației (NIS)[3], care urmează a fi adoptată în curând – precum și Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice constituie, până în prezent, esența răspunsului politic al Uniunii Europene la aceste provocări de securitate cibernetică. În plus, UE are la dispoziție entități specializate, cum ar fi Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol și Centrul de răspuns la incidente de securitate cibernetică (CERT-UE). Recent, au fost lansate, de asemenea, o serie de inițiative sectoriale (de exemplu, în sectoarele energiei și transporturilor) pentru a spori securitatea cibernetică în diferite sectoare critice.

În pofida acestor rezultate pozitive, UE rămâne vulnerabilă la incidentele cibernetice. Acest lucru ar putea submina piața unică digitală și viața economică și socială în ansamblu. Impactul acestora poate să nu se limiteze doar la domeniul economiei. În cazul amenințărilor hibride[4], atacurile informatice pot fi utilizate într-o manieră coordonată cu alte activități pentru a destabiliza o țară sau pentru a pune în dificultate instituțiile politice.

În acest context, gestionarea incidentelor cibernetice de mare amploare, care implică mai multe state membre simultan ar putea reprezenta o provocare pentru UE. În sinergie cu comunicarea privind contracararea amenințărilor hibride și, respectiv, cu comunicarea privind punerea în aplicare a Agendei europene privind securitatea[5], Comisia analizează modalitățile de a aborda realitatea în schimbare în materie de securitate cibernetică și evaluează măsurile suplimentare care ar putea fi necesare pentru îmbunătățirea rezilienței și a răspunsului UE la incidentele de securitate cibernetică.

În plus, Comisia abordează, de asemenea, capacitățile industriale în domeniul securității cibernetice în UE. Deși întregul lanț valoric al tehnologiilor digitale nu poate fi ținut sub control în Europa, este nevoie cel puțin de menținerea și dezvoltarea anumitor capacități

[1] *Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II; Center for Strategic and International Studies* (Pierderi nete: estimarea costurilor globale ale infracționalității cibernetice – impactul economic al infracționalității cibernetice II, Centrul pentru studii strategice și internaționale)*;* iunie *2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

esențiale. Furnizarea de produse și servicii care asigură cel mai ridicat nivel de securitate cibernetică reprezintă o oportunitate pentru sectorul securității cibernetice în Europa și ar putea deveni un puternic avantaj competitiv. Se estimează că piața globală a securității cibernetice se va număra printre segmentele cu creșterea cea mai rapidă din sectorul TIC[6]. Transformarea UE într-un actor principal în acest domeniu trebuie să fie sprijinită de o puternică cultură a securității datelor, inclusiv a datelor cu caracter personal, precum și de un răspuns eficace în caz de incidente. Aceasta va fi privită ca un argument puternic pentru a investi în UE, contribuind astfel la realizarea obiectivelor ambițioase ale pieței unice digitale, pentru a genera creștere economică și locuri de muncă.

Este nevoie de un angajament puternic pentru a realiza deziderateleе de mai sus, în special prin:

i) intensificarea cooperării în vederea îmbunătățirii pregătirii și a răspunsului la incidentele cibernetice

Mecanismele de cooperare existente și convenite trebuie să fie consolidate pentru a spori reziliența și gradul de pregătire al UE, inclusiv pentru o eventuală criză paneuropeană de securitate cibernetică. Aceste mecanisme de cooperare ar trebui să fie cuprinzătoare și să acopere ciclul de viață al unui incident, de la prevenire la urmărirea penală. Cooperarea eficace dintre statele membre și punerea în practică a cerințelor de securitate pentru operatorii esențiali vor necesita, de asemenea, soluții tehnice robuste de securitate cibernetică din partea sectorului securității cibernetice.

În același timp, asigurarea rezilienței activelor cibernetice esențiale din întreaga UE va necesita eforturi continue pentru a se găsi sinergii intersectoriale și pentru a se integra cerințele de securitate cibernetică în toate politicile relevante ale UE. În viitorul apropiat, Comisia va examina necesitatea actualizării strategiei de securitate cibernetică a UE din 2013.

ii) Abordarea provocărilor cu care se confruntă piața unică a securității cibernetice din Europa

Strategia pieței unice digitale [7] a recunoscut că există încă lacune specifice în domeniul cu evoluție rapidă al tehnologiilor și al soluțiilor pentru securitatea rețelelor online. În același timp, studiile de piață arată că piața internă a UE este încă fragmentată din punct de vedere geografic în ceea ce privește furnizarea de produse și servicii de securitate cibernetică[8]. Prezenta comunicare stabilește o serie de măsuri de politică orientate către piață, pentru a aborda aceste lacune și provocări ale pieței unice.

iii) Dezvoltarea capabilităților industriale în domeniul securității cibernetice

În Strategia de securitate cibernetică a UE și în Strategia privind piața unică digitală, Comisia s-a angajat să promoveze creșterea ofertei de produse și servicii ale sectorului UE al securității cibernetice. Prin urmare, Comisia adoptă, de asemenea, o decizie care să deschidă calea către un parteneriat public-privat contractual (PPPc) privind securitatea cibernetică, care

[6] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.
[7] COM(2015) 192.
[8] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.

urmărește să promoveze o agendă de cercetare și inovare europeană de vârf în materie de securitate cibernetică pentru creșterea competitivității.

2. DEZVOLTAREA COOPERĂRII, A CUNOȘTINȚELOR ȘI A CAPACITĂȚILOR LA UN NIVEL SUPERIOR

Strategia UE de securitate cibernetică și, în special, viitoarea Directivă NIS[9] vor deschide calea spre îmbunătățirea cooperării la nivelul UE între statele membre. Punerea în aplicare rapidă și eficace a directivei va fi esențială, având în vedere digitizarea crescândă a vieții economice și sociale (luând în considerare, de asemenea, cloudul, internetul obiectelor și comunicarea directă între calculatoare), creșterea interconectării transfrontaliere și evoluția rapidă a peisajului amenințărilor cibernetice[10]. În acest context, UE trebuie să se pregătească pentru eventualitatea apariției unei crize cibernetice de anvergură[11], inclusiv, de exemplu, atacuri simultane împotriva sistemelor informaționale critice, în mai multe state membre[12].

Cooperarea la nivelul UE este, prin urmare, esențială pentru abordarea atât a incidentelor cibernetice inițial la scară mai mică, dar cu potențial de proliferare, cât și a unui eventual atac pe scară largă în mai multe state membre. UE trebuie să integreze aspectele cibernetice în mecanismele existente de gestionare a crizelor. De asemenea, UE trebuie să asigure o cooperare eficace și mecanisme de schimb rapid de informații între sectoare și între statele membre pentru a răspunde unor astfel de incidente și pentru a împiedica propagarea efectelor acestora. În plus, aceste mecanisme ar trebui să funcționeze în mod coerent, contribuind astfel la lupta împotriva terorismului, a criminalității organizate și a criminalității informatice. Acest lucru ar spori totodată capacitatea UE de a-și coordona acțiunile cu partenerii săi internaționali pentru a răspunde în mod eficace la amenințări și incidente.

2.1. Valorificarea la maximum a mecanismelor de cooperare în domeniul NIS și trecerea la ENISA 2.0

O parte esențială a capacităților naționale impuse de directiva NIS sunt echipele de intervenție în caz de incidente informatice (*Computer Incident Response Teams* - CSIRT) responsabile de reacția rapidă la amenințările și la incidentele cibernetice. Acestea vor constitui rețeaua CSIRT, în vederea promovării unei cooperări operaționale eficace cu privire la anumite incidente de securitate cibernetică și a schimbului de informații privind riscurile. În plus, directiva va crea un grup de cooperare pentru a sprijini și facilita cooperarea strategică dintre statele membre și consolidarea încrederii între acestea.

Având în vedere natura și multitudinea amenințărilor cibernetice, Comisia încurajează statele membre să valorifice la maximum mecanismele de cooperare în domeniul NIS și să consolideze cooperarea transfrontalieră legată de pregătirea în caz de incidente cibernetice de mare amploare. O astfel de cooperare suplimentară cu privire la incidentele cibernetice

[9] Directiva NIS va impune statelor membre să identifice o serie de operatori de servicii esențiale în domenii cum ar fi energia, transporturile, finanțele și sănătatea, pentru a aborda riscurile privind securitatea cibernetică și pentru a asigura, totodată, că anumiți furnizori de servicii digitale iau măsurile adecvate pentru a răspunde acestor riscuri.
[10] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.
[11] A se vedea, de exemplu, raportul ENISA: Practici comune la nivelul UE de gestionare a crizelor și aplicabilitatea la crizele cibernetice (aprilie 2016).
[12] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.

semnificative ar avea de câștigat de pe urma unei abordări coordonate a cooperării în situații de criză între diferitele elemente ale ecosistemului cibernetic. O astfel de abordare poate fi prezentată sub forma unui „plan”, care ar asigura, de asemenea, sinergiile și coerența cu mecanismele existente de gestionare a crizelor[13]. Pe de altă parte, această abordare ar trebui testată în mod periodic în cadrul exercițiilor de gestionare a crizelor în materie de criminalitate informatică și a altor tipuri de crize. Aceasta ar include un rol pentru organisme de la nivelul UE, cum ar fi ENISA, CERT-UE și Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol, precum și utilizarea instrumentelor dezvoltate în contextul rețelei CSIRT. În prima jumătate a anului 2017, Comisia va prezenta un astfel de plan de cooperare pentru a fi examinat de grupul de cooperare, de rețeaua CSIRT și de alte părți interesate relevante.

În prezent, sunt disponibile la nivelul UE cunoștințe și expertiză cu privire la securitatea cibernetică, însă într-un mod dispersat și nestructurat. Pentru sprijinirea mecanismelor de cooperare în domeniul NIS, informațiile ar trebui reunite într-o „platformă de informare” (*information hub*) pentru a fi ușor disponibile la cerere în toate statele membre. Această platformă ar deveni o resursă esențială care ar permite instituțiilor UE și statelor membre să facă schimb de informații, după caz. Facilitarea accesului la informații mai bine structurate privind riscurile de securitate cibernetică și potențialele măsuri corective ar trebui să ajute statele membre să își consolideze capacitățile, să își alinieze practicile și să își îmbunătățească, astfel, reziliența generală la atacuri. Comisia, cu sprijinul ENISA, al CERT-UE și cu expertiza Centrului său Comun de Cercetare, va facilita crearea și asigurarea sustenabilității platformei.

În plus, ar trebui constituit la nivelul UE un grup consultativ la nivel înalt privind securitatea cibernetică, cu o componență fixă și care să se întrunească periodic[14], ,alcătuit din experți și factori de decizie din industrie, mediul academic, societatea civilă și alte organizații relevante. Grupul va permite Comisiei să beneficieze, într-un mod deschis și transparent, de expertiza și contribuțiile externe în ceea ce privește politicile sale legate de strategia privind securitatea cibernetică și posibilele măsuri de reglementare sau alte acțiuni de politici publice. Acesta ar completa acțiunea altor structuri active în domeniul securității cibernetice și ar asigura legătura cu acestea[15].

În plus, Comisia are obligația de a evalua ENISA până la 20 iunie 2018, iar eventuala modificare sau reînnoire a mandatului ENISA trebuie adoptată până la 19 iunie 2020[16]. Având în vedere situația actuală în materie de securitate cibernetică, Comisia își propune să devanseze această evaluare și, în funcție de rezultatele acesteia, să prezinte o propunere cât mai curând posibil.

[13] În special mecanismele integrate pentru răspuns politic la crize, inclusiv decizia privind modalitățile de punere în aplicare de către Uniune a clauzei de solidaritate (24 iulie 2014) și procesele decizionale din cadrul politicii de securitate și apărare comune.

[14] Grupurile de experți ale Comisiei sunt supuse normelor orizontale instituite prin Decizia C(2016)3301 a Comisiei.

[15] De exemplu, platforma NIS, parteneriatul public-privat contractual privind securitatea cibernetică și platformele sectoriale cum ar fi platforma experților în materie de securitate cibernetică din sectorul energiei (EECSP). De asemenea, ar trebui să asigure corelarea cu concluziile mesei rotunde la nivel înalt anunțate în Comunicarea privind digitalizarea industriei europene: COM(2016) 180 final.

[16] Regulamentul (UE) nr. 526/2013 de abrogare a Regulamentului (CE) nr. 460/2004.

La evaluarea eventualei necesități de se modifica mandatul ENISA, Comisia va lua în considerare provocările în materie de securitate cibernetică descrise mai sus și efortul global de intensificare a cooperării și a schimbului de cunoștințe. Acest proces va oferi ocazia de a examina necesitatea eventuală de consolidare a capabilităților și a capacităților agenției de a sprijini statele membre în mod durabil în realizarea rezilienței cibernetice. Reflecția cu privire la mandatul ENISA ar trebui să țină seama, totodată, de noile responsabilități ale agenției, în temeiul Directivei privind securitatea rețelelor și a informației („Directiva NIS"), de noile obiective strategice de sprijinire a sectorului securității cibernetice (Strategia privind piața unică digitală și, în special, PPPc), de evoluția necesităților în ceea ce privește securizarea sectoarelor critice și de noile provocări legate de incidente transfrontaliere, inclusiv de necesitatea de a oferi un răspuns coordonat la crizele cibernetice.

Comisia:

- va prezenta spre examinare un plan de cooperare pentru gestionarea incidentelor cibernetice de mare amploare la nivelul UE, în prima jumătate a anului 2017;
- va facilita crearea unei „platforme de informare" pentru a sprijini schimbul de informații dintre organismele UE și statele membre;
- va crea un grup consultativ la nivel înalt privind securitatea cibernetică și
- va finaliza evaluarea ENISA până la sfârșitul anului 2017. Această evaluare va aborda necesitatea modificării sau extinderii mandatului ENISA, în vederea unei eventuale propuneri, cât mai curând posibil.

2.2 Sporirea eforturilor în ceea ce privește educarea, formarea și exercițiile în domeniul securității cibernetice

Competențele și formarea adecvate, atât pentru prevenirea incidentelor de securitate cibernetică, cât și pentru abordarea și atenuarea efectelor acestora, sunt câteva dintre principalele aspecte legate de realizarea rezilienței cibernetice.

În prezent, ENISA, Grupul european de formare și educație în combaterea criminalității informatice (ECTEG), în cooperare cu Centrul european de combatere a criminalității informatice din cadrul Europol și cu Colegiul European de Poliție (CEPOL), joacă un rol important în furnizarea de sprijin pentru consolidarea capacităților cibernetice – inclusiv cu privire la criminalistica cibernetică – prin elaborarea de manuale și organizarea de cursuri de formare și de exerciții de securitate cibernetică.

În același timp, spațiul cibernetic este un domeniu în rapidă evoluție, în care capacitățile cu dublă utilizare joacă un rol esențial. Prin urmare, este necesar să se dezvolte cooperarea civilo-militară și sinergiile în materie de formare și exerciții pentru a spori reziliența și capacitățile UE de răspuns la incidente.

Pentru a răspunde acestei necesități, și ca urmare a adoptării Directivei NIS și a cadrului de politici pentru apărarea cibernetică a UE[17], serviciile Comisiei vor coopera cu statele membre,

[17] Adoptat de Consiliul Afaceri Externe al Uniunii Europene din 18 noiembrie 2014, doc. 15585/14.

cu Serviciul European de Acțiune Externă (SEAE), cu ENISA și cu alte organisme relevante ale UE[18] pentru a stabili o platformă de educare, exerciții și formare privind securitatea cibernetică, care va promova sinergiile dintre formarea oferită în sectorul civil și cea din sectorul de apărare.

Comisia:

- va lucra în strânsă cooperare cu statele membre, SEAE, ENISA și cu alte organisme competente ale UE pentru a institui o platformă de formare în materie de securitate cibernetică.

2.3. Abordarea interdependențelor intersectoriale și a rezilienței infrastructurii rețelelor publice majore

Un factor important în evaluarea riscurilor și a impactului incidentelor cibernetice de mare amploare este gradul de interdependență la nivel transfrontalier și transsectorial. Un incident cibernetic grav într-un sector sau într-un stat membru poate avea, direct sau indirect, un impact asupra altor sectoare sau a altor state membre sau se poate propaga către acestea.

Cooperarea transfrontalieră și transsectorială, facilitează schimbul de informații și de expertiză și, astfel, contribuie la creșterea gradului de pregătire și a rezilienței. Comisia a sprijinit eforturile din diferite sectoare pentru o mai bună înțelegere a interdependențelor prin punerea în aplicare a programului european privind protecția infrastructurilor critice[19].

În același timp, o condiție prealabilă necesară pentru abordarea riscurilor intersectoriale este capacitatea fiecărui sector în parte de a identifica incidentele cibernetice, de a se pregăti pentru acestea și de a acționa în cazul în care au loc. Comisia va evalua riscurile care decurg din incidentele cibernetice în sectoarele cu un grad ridicat de interdependență în interiorul și în afara frontierelor naționale, în special în ceea ce privește sectoarele acoperite de Directiva NIS, ținând seama, de asemenea, de evoluțiile pe plan internațional[20]. Pe baza acestei evaluări, Comisia va analiza dacă este nevoie de mai multe norme specifice și/sau de orientări privind pregătirea pentru a răspunde riscurilor legate de securitatea cibernetică pentru aceste sectoare critice.

La nivel european, centrele sectoriale de schimb și analiză de informații[21] (ISAC) și centrele corespunzătoare CSIRT pot juca un rol-cheie în pregătirea pentru incidentele cibernetice și pentru răspunsul la acestea. Pentru a asigura o circulație eficace a informațiilor privind evoluția amenințărilor și pentru a facilita răspunsul la incidentele cibernetice, centrele ISAC ar trebui să fie încurajate să colaboreze cu rețeaua CSIRT în temeiul Directivei NIS, cu Centrul european de combatere a criminalității informatice din cadrul Europol, CERT-UE și cu organismele competente de aplicare a legii.

[18] Cum ar fi Colegiul European de Securitate și Apărare, EC3, CEPOL și Agenția Europeană de Apărare.
[19] Documentul de lucru al serviciilor Comisiei SWD (2013) 318.
[20] De exemplu, foaia de parcurs privind securitatea cibernetică, adoptată de Agenția Europeană de Siguranță a Aviației, și activitatea Organizației Aviației Civile Internaționale și a Organizației Maritime Internaționale.
[21] A se vedea, de exemplu, centrul european ISAC din sectorul energiei (http://www.ee-isac.eu).

Schimbul de informații dintre părțile interesate și cu autoritățile pe durata de viață a riscurilor cibernetice necesită ca participanții să aibă asigurarea că răspunderea lor nu va fi angajată ca urmare a acestor schimburi de informații. Comisia a remarcat o serie de astfel de îngrijorări care împiedică întreprinderile să facă schimb de informații prețioase cu omologii lor cu privire la amenințări, în cadrul sectoarelor sau cu autoritățile, în special la nivel transfrontalier. Comisia va căuta să abordeze și să îndepărteze astfel de preocupări în interesul îmbunătățirii schimbului de informații cu privire la amenințările cibernetice.

Canalele de raportare sigure care garantează confidențialitatea sunt, de asemenea, vitale pentru a încuraja întreprinderile să raporteze furtul cibernetic de secrete comerciale. Acest lucru ar facilita monitorizarea și evaluarea prejudiciului suferit de industria europeană (care a condus, totodată la scăderea vânzărilor și a ocupării forței de muncă) și de organismele de cercetare. Acest lucru ar contribui, de asemenea, la elaborarea unui răspuns politic adecvat. Cu sprijinul ENISA, al Oficiului Uniunii Europene pentru Proprietatea Intelectuală (EUIPO) și al EC3 din cadrul Europol, Comisia va stabili — pe baza dialogului cu părțile interesate din sectorul privat — canale sigure pentru raportarea voluntară a furtului cibernetic de secrete comerciale. Acest fapt ar trebui să facă posibilă colectarea de date anonimizate și agregate la nivelul UE. Aceste date pot fi partajate cu statele membre pentru a fi utilizate în eforturile diplomatice și în acțiunile de sensibilizare menite să contribuie la protejarea activelor necorporale ale UE de atacurile cibernetice.

Pentru a sprijini securitatea cibernetică sectorială, Comisia va promova, de asemenea, integrarea securității cibernetice în elaborarea diverselor politici sectoriale ale UE în care securitatea cibernetică este o miză.

În cele din urmă, dar nu în ultimul rând, autoritățile publice au de jucat un rol în verificarea integrității infrastructurilor esențiale de internet pentru a detecta problemele, pentru a informa partea responsabilă de aceste rețele și – oriunde este necesar – pentru a furniza asistență pentru remedierea vulnerabilităților cunoscute. Autoritățile naționale de reglementare ar putea utiliza capacitățile CSIRT pentru a efectua examinări periodice ale infrastructurilor rețelelor publice. Pe această bază, ele ar putea încuraja operatorii să remedieze lacunele sau să abordeze vulnerabilitățile pe care aceste examinări le-ar putea identifica.

Prin urmare, Comisia va examina condițiile juridice și organizatorice necesare pentru a permite autorităților naționale de reglementare, în cooperare cu autoritățile naționale din domeniul securității cibernetice, să solicite CSIRT-urilor să efectueze în mod periodic controale privind vulnerabilitatea infrastructurilor rețelelor publice. CSIRT naționale ar trebui încurajate să coopereze în cadrul rețelei CSIRT cu privire la cele mai bune practici în ceea ce privește monitorizarea, facilitând astfel prevenirea unor incidente de mare amploare.

Comisia:

- va promova dezvoltarea cooperării europene a centrelor sectoriale de schimb și analiză de informații, va sprijini colaborarea acestora cu CSIRT-urile și va urmări să abordeze obstacolele care ar putea împiedica participanții de pe piață să schimbe informații;
- va studia riscurile strategice/sistemice care decurg din incidentele cibernetice din

sectoarele foarte interdependente din interiorul frontierelor naționale și dincolo de acestea;
- va evalua necesitatea unor norme și/sau orientări suplimentare referitoare la gradul de pregătire pentru a răspunde riscurilor legate de securitatea cibernetică în sectoarele critice și, după caz, va reflecta asupra conținutului lor;
- va institui, împreună cu ENISA, EUIPO și EC3 canale fiabile pentru raportarea voluntară a furturilor cibernetice de secrete comerciale;
- va promova integrarea măsurilor de securitate cibernetică în politicile sectoriale europene și
- va examina condițiile necesare pentru a permite autorităților naționale să solicite CSIRT-urilor efectuarea unor verificări periodice ale infrastructurilor rețelelor majore.

3. ABORDAREA PROVOCĂRILOR CU CARE SE CONFRUNTĂ PIAȚA UNICĂ A SECURITĂȚII CIBERNETICE ÎN EUROPA

Europa are nevoie de produse și soluții de securitate cibernetică de înaltă calitate, accesibile și interoperabile. Cu toate acestea, oferta de produse și servicii de securitate în sectorul TIC din cadrul pieței unice rămâne foarte fragmentată din punct de vedere geografic. Pe de o parte, acest lucru îngreunează concurența întreprinderilor europene la nivel național, european și mondial, iar pe de altă parte, reduce posibilitățile de alegere a tehnologiilor de securitate cibernetică viabile și utilizabile la care au acces[22] cetățenii și întreprinderile.

Într-adevăr, sectorul securității cibernetice din Europa s-a dezvoltat de-a lungul timpului în principal pe baza cererii guvernamentale naționale, inclusiv în sectorul apărării. Cei mai mulți dintre contractanții din sectorul european al apărării au instituit departamente de securitate cibernetică[23]. În paralel, au apărut o multitudine de IMM-uri inovatoare, în special pe piețele specializate/pe nișele de piață (de exemplu, sistemele criptografice) și pe piețe bine stabilite cu noi modele de afaceri (de exemplu, programele antivirus).

Cu toate acestea, întreprinderile au dificultăți din ce în ce mai mari în afara pieței lor interne, naționale. Lipsa de încredere în soluțiile oferite în mod „transfrontalier” este factorul esențial pe care l-au relevat în mod clar toate consultările realizate de Comisie[24]. În consecință, multe dintre achizițiile publice se desfășoară încă la nivelul unui stat membru dat și numeroase întreprinderi depun eforturi susținute pentru a realiza economiile de scară ce le-ar permite să fie mai competitive atât pe piața internă, cât și la nivel mondial.

Lipsa de soluții interoperabile (standarde tehnice), de practici (standarde procesuale) și de mecanisme de certificare la nivelul UE este una dintre lacunele care afectează piața unică în domeniul securității cibernetice. În acest context securitatea cibernetică a fost identificată ca fiind una dintre prioritățile de standardizare din sectorul TIC pentru piața unică digitală[25].

[22] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.
[23] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.
[24] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 215.
[25] COM(2016) 176/2.

Perspectivele limitate de creștere pentru societățile cu activitate în sectorul securității cibernetice în interiorul pieței unice conduc la o multitudine de fuziuni și achiziții de către investitori din afara Europei[26]. Această tendință demonstrează capacitatea de inovare a antreprenorilor europeni din domeniul securității cibernetice însă, în același timp, există și riscul pierderii de know-how și expertiză europeană, precum și al unui exod de creiere.

Sunt necesare acțiuni urgente pentru promovarea unei piețe unice mai integrate pentru produse și servicii de securitate cibernetică care să faciliteze dezvoltarea de soluții mai practice și mai accesibile.

Barierele de încredere în rândul actorilor industriali și instituționali europeni pot fi depășite prin favorizarea cooperării la începutul ciclului de viață al inovării: atât la nivelul sectorului securității cibernetice, între furnizori și cumpărători, cât și la nivel intersectorial unde sunt implicate sectoare care sunt deja sau pot deveni clienți pentru soluțiile de securitate cibernetică.

În același timp, dezvoltarea de produse, servicii și tehnologii cu dublă utilizare devine din ce în ce mai importantă în Europa. Un număr din ce în ce mai mare de soluții sunt introduse de pe piața civilă pe piața din domeniul apărării[27]. În viitorul plan de acțiune european în domeniul apărării, Comisia intenționează să identifice măsuri suplimentare pentru a stimula sinergiile dintre domeniile civil și militar la nivel european.

3.1 Certificare și etichetare

Certificarea joacă un rol important în ceea ce privește creșterea securității produselor și a serviciilor și a încrederii în acestea. Acest lucru este valabil și pentru acele sisteme noi care folosesc pe scară largă tehnologiile digitale și care necesită un nivel înalt de securitate, precum autovehiculele conectate și automatizate, dispozitivele electronice pentru sănătate, sistemele industriale de automatizare și control (SIGA) sau rețelele inteligente.

Se dezvoltă inițiative naționale menite să stabilească cerințe de securitate cibernetică la nivel înalt pentru componentele infrastructurii TIC tradiționale, inclusiv cerințe de certificare. Deși importante, acestea prezintă riscul de a conduce la fragmentarea pieței interne și la dificultăți legate de interoperabilitate. Doar în câteva state membre există sisteme de certificare a securității eficace pentru produsele TIC[28]. Prin urmare, este posibil ca un furnizor de TIC să trebuiască să se supună mai multor proceduri de certificare pentru a putea să vândă în mai multe state membre. În scenariul cel mai nefavorabil, un produs sau un serviciu TIC conceput pentru a îndeplini cerințele de securitate cibernetică dintr-un stat membru nu poate fi comercializat într-un alt stat membru.

În scopul realizării unei piețe unice funcționale în domeniul securității cibernetice, un eventual cadru de certificare a produselor și serviciilor TIC ar trebui să urmărească atingerea următoarelor obiective: (i) acoperirea unei game mai largi de sisteme, produse și servicii TIC,

[26] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.
[27] În 2013, domeniul exporturilor de produse cu dublă utilizare reprezenta deja aproximativ 20 % din exporturile totale ale UE (ca valoare). Aceasta include comerțul în interiorul UE.
[28] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216 pentru Grupul înalților funcționari pentru acordul privind sistemele informatice [Decizia Consiliului din 31 martie 1992 (92/242/CEE)] și alte sisteme existente, cum ar fi *Commercial Product Assurance* în Regatul Unit, *Certification Sécuritaire de Premier Niveau* în Franța.

(ii) asigurarea punerii sale în aplicare în toate cele 28 de state membre și (iii) abordarea oricărui nivel de securitate cibernetică, luând în același timp în considerare evoluțiile la nivel internațional.

În acest scop, Comisia va înființa un grup de lucru specific privind certificarea securității produselor și serviciilor TIC, alcătuit din experți din partea statelor membre și a industriei. Obiectivul acestuia va fi de a dezvolta, în cooperare cu ENISA și Centrul Comun de Cercetare, până la sfârșitul anului 2016, o foaie de parcurs care să studieze posibilitatea de a se elabora, până la sfârșitul anului 2017, o propunere pentru un astfel de cadru european de certificare de securitate în domeniul TIC. În acest context, Comisia va examina, de asemenea, Regulamentul (CE) nr. 2008/765 și dispozițiile privind certificarea cuprinse în Regulamentul general privind protecția datelor nr. 2016/679[29].

Procesul va include o amplă consultare și o evaluare a impactului. Acest lucru va permite Comisiei să examineze diferite opțiuni pentru crearea unui cadru de certificare a produselor și serviciilor TIC. Comisia va examina, de asemenea, certificarea securității TIC în sectoarele de infrastructură (de exemplu în sectorul transportului aerian, feroviar, al automobilelor), precum și în mecanismele specifice de certificare și validare a tehnologiei „ready-to-be-deployed" („gata pentru a fi utilizată") (de exemplu, securitatea cibernetică a sistemelor industriale de automatizare și control[30], internetul obiectelor, cloud). De asemenea, aceasta va aborda lacunele identificate în cadrul sistemului european de certificare de securitate a TIC menționat mai sus.

Pe cât posibil, eforturile de certificare se vor baza pe standarde recunoscute la nivel internațional și vor fi dezvoltate cu parteneri internaționali.

Comisia va studia, de asemenea, opțiunile legate de modalitatea optimă de a integra certificarea securității TIC în viitoarea legislație sectorială de certificare, care include și aspecte legate de siguranță.

Pe lângă eventualele opțiuni de reglementare, Comisia va examina, de asemenea, crearea unui sistem european de etichetare ce nu implică o sarcină administrativă prea împovărătoare, pe bază voluntară și de orientare comercială, privind securitatea produselor TIC. Acest sistem va veni în completarea certificării și va avea drept scop sporirea gradului de vizibilitate a securității cibernetice în produsele comerciale astfel încât să crească competitivitatea acestora atât în cadrul pieței unice, cât și la nivel mondial. O atenție corespunzătoare va fi acordată inițiativelor orizontale și sectoriale în curs lansate de industrie, atât la nivelul ofertei, cât și la nivelul cererii.

Administrațiile publice vor fi implicate îndeaproape pentru a permite utilizarea unor specificații și referințe comune privind certificarea în contextul achizițiilor publice. De asemenea, Comisia va monitoriza și va raporta cu privire la utilizarea cerințelor relevante în

[29] Regulamentul (UE) nr. 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date prevede două coduri de conduită menite să contribuie la aplicarea corespunzătoare a normelor privind protecția datelor, precum și mecanisme de certificare ce acoperă toate principiile de protecție a datelor, în special în ceea ce privește securitatea prelucrării datelor cu caracter personal.

[30] A se vedea grupul tematic al ERNCIP privind „Securitatea cibernetică a sistemelor industriale de control", disponibil la adresa https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

materie de certificare în domeniul achizițiilor publice la nivel național, în special pentru sistemele sectoriale (energie, transporturi, sănătate, administrație publică etc.).

Comisia:

- va elabora, până la sfârșitul anului 2016, o foaie de parcurs în vederea elaborării unei propuneri pentru un posibil cadru european de certificare de securitate în domeniul TIC, propunere care ar urma să fie prezentată până la sfârșitul anului 2017, și va evalua fezabilitatea și impactul unui cadru european de etichetare în ceea ce privește securitatea cibernetică ce nu implică o sarcină administrativă prea împovărătoare;
- va examina necesitatea și, dacă este cazul, va remedia lacunele existente în certificarea de securitate în domeniul TIC în cadrul actualelor mecanisme sectoriale de certificare/validare;
- va asigura, după caz, integrarea certificării securității produselor TIC în viitoarele propuneri legislative sectoriale;
- va stimula implicarea administrațiilor publice pentru a facilita utilizarea certificării și a specificațiilor comune în contextul achizițiilor publice și
- va monitoriza utilizarea cerințelor relevante în materie de certificare în achizițiile publice și comerciale și va prezenta, peste trei ani, un raport cu privire la situația pieței.

3.2. Trecerea la o viteză superioară în ceea ce privește investițiile în materie de securitate cibernetică în Europa și sprijinirea IMM-urilor

Într-un moment în care inovarea în sectorul securității cibernetice cunoaște o creștere spectaculoasă în Europa, la nivelul UE nu există încă o cultură suficient de dezvoltată a investițiilor în securitatea cibernetică. Există multe IMM-uri inovatoare în domeniu, dar acestea sunt adesea incapabile să își intensifice activitățile. Acest lucru se întâmplă, printre altele, din cauza lipsei unei finanțări ușor accesibile pentru a le sprijini în fazele incipiente de dezvoltare. De asemenea, întreprinderile au acces limitat la capitalul de risc în Europa, iar bugetul disponibil pentru marketing, pentru a le îmbunătăți vizibilitatea sau pentru asigurarea respectării diferitelor seturi de standarde și cerințe de conformitate, este inadecvat.

În același timp, cooperarea dintre actorii de securitate cibernetică este destul de fragmentată și sunt necesare eforturi suplimentare pentru a spori concentrarea economică și pentru a dezvolta noi lanțuri ale valorii[31].

Pentru intensificarea investițiilor în domeniul securității cibernetice în Europa și pentru sprijinirea IMM-urilor, este necesară facilitarea accesului IMM-urilor la finanțare. Trebuie să existe, de asemenea, sprijin pentru dezvoltarea unor clustere și centre de excelență competitive la nivel mondial în materie de securitate cibernetică în ecosisteme regionale favorabile dezvoltării digitale. Acest sprijin trebuie să fie legat de punerea în aplicare a unor

[31] A se vedea documentul de lucru al serviciilor Comisiei SWD(2016) 216.

strategii de specializare inteligentă și a altor instrumente ale UE, astfel încât sectorul securității cibernetice din Europa să poată profita mai bine de avantajele oferite de acestea.

Abordarea Comisiei va fi aceea de a optimiza gradul de informare a comunității de securitate cibernetică cu privire la oportunitățile de finanțare la nivel european, național și regional (în ceea ce privește atât instrumentele orizontale, cât și cererile de propuneri specifice[32]) prin utilizarea instrumentelor și a canalelor existente, cum ar fi *Enterprise Europe Network*.

Comisia va completa aceste eforturi examinând, împreună cu Banca Europeană de Investiții (BEI) și cu Fondul European de Investiții (FEI), modalitățile de facilitare a accesului la finanțare. Acest lucru se poate realiza fie sub formă de investiții de capital și de cvasicapital, împrumuturi, garanții pentru proiecte sau contragaranții pentru intermediari, de exemplu prin crearea unei platforme de investiții pentru securitatea cibernetică în cadrul Fondului european pentru investiții strategice[33].

În plus, Comisia va examina, la rândul său, posibilitatea dezvoltării, împreună cu statele membre și regiunile interesate, a unei platforme de specializare inteligentă în materie de securitate cibernetică[34]. Acest lucru ar ajuta la coordonarea și planificarea strategiilor de securitate cibernetică și la instituirea unei colaborări strategice a părților interesate de ecosistemele regionale. Această abordare ar trebui, de asemenea, să contribuie la deblocarea potențialului fondurilor structurale și de investiții europene existente pentru sectorul securității cibernetice.

La un nivel mai general, Comisia va promova o abordare prin care elementele de securitate sunt incluse încă de la nivelul de proiect. Aceasta va căuta să se asigure că cerințele de securitate cibernetică sunt abordate în mod consecvent în toate proiectele majore de investiții în infrastructuri care au o componentă digitală și care sunt cofinanțate de fondurile europene. Acest lucru va fi realizat prin introducerea treptată a cerințelor relevante în normele privind achizițiile publice și în normele programului.

Comisia:

- va utiliza instrumentele existente de sprijinire a IMM-urilor pentru a sensibiliza publicul în legătură cu mecanismele de finanțare existente în cadrul comunității de securitate cibernetică;
- va continua intensificarea utilizării instrumentelor și mecanismelor UE pentru sprijinirea IMM-urilor inovatoare în ceea ce privește explorarea sinergiilor dintre piețele securității cibernetice civile și de apărare[35];
- va explora împreună cu BEI și FEI fezabilitatea facilitării accesului la investiții, de

[32] A se vedea, de exemplu, cererea de propuneri multisectorială pentru 2016 din cadrul Mecanismului pentru interconectarea Europei și cererile de propuneri COSMO 2016 legate de programul de internaționalizare a clusterelor.

[33] În cadrul Fondului european pentru investiții strategice, proiectele individuale pot fi sprijinite, direct sau indirect, prin intermediul unor platforme de investiții. Astfel de platforme pot contribui la finanțarea proiectelor mai mici și pot reuni fonduri din diferite surse pentru a permite investiții diversificate cu orientare geografică sau tematică.

[34] A se vedea instrumentele de specializare inteligentă (RIS3): http://s3platform.jrc.ec.europa.eu/.

[35] De exemplu, *Enterprise Europe Network* și *European Network of Defence-related Regions* vor oferi regiunilor noi oportunități de explorare a cooperării transfrontaliere în domeniul produselor cu dublă utilizare, inclusiv în materie de securitate cibernetică, iar IMM-urilor le vor oferi posibilitatea de a explora parteneriate potențiale .

exemplu, prin intermediul unei platforme specializate de investiții pentru securitatea cibernetică sau al altor instrumente de securitate cibernetică;
- va dezvolta o platformă specializată inteligentă pentru securitatea cibernetică pentru a sprijini statele membre și regiunile interesate să investească în sectorul securității cibernetice (RIS3) și
- va promova o abordare prin care elementele de securitate sunt incluse încă de la nivelul de proiect în investițiile majore în infrastructuri care au o componentă digitală și sunt cofinanțate din fonduri UE.

4. STIMULAREA ȘI ÎNCURAJAREA PRIN INOVARE A SECTORULUI EUROPEAN AL SECURITĂȚII CIBERNETICE — INSTITUIREA PARTENERIATULUI PUBLIC-PRIVAT CONTRACTUAL PRIVIND SECURITATEA CIBERNETICĂ (PPPC)

În scopul stimulării competitivității și inovării în sectorul european al securității cibernetice, va fi semnat un parteneriat public-privat contractual (PPPc) privind securitatea cibernetică. PPPc va reuni resursele publice și industriale pentru obținerea excelenței în cercetare și inovare.

PPPc are scopul de a construi încrederea între statele membre și actorii industriali prin promovarea cooperării încă din primele etape ale procesului de cercetare și inovare. Acesta urmărește, de asemenea, să contribuie la alinierea sectoarelor aferente cererii și ofertei. Acest lucru ar trebui să îi permită industriei să obțină cerințele viitoare de la utilizatorii finali și de la sectoarele care sunt clienți importanți pentru soluțiile de securitate cibernetică (de exemplu, energie, sănătate, transporturi, finanțe) și va facilita implicarea acestora din urmă în definirea cerințelor comune privind securitatea digitală, protecția vieții private și a datelor pentru sectoarele lor.

Parteneriatul public-privat contractual privind securitatea cibernetică va permite, de asemenea, o utilizare la maximum a fondurilor disponibile. Acest lucru va fi realizat în primul rând printr-o mai bună coordonare cu statele membre. În al doilea rând, va exista o concentrare mai bună asupra unui număr restrâns de priorități tehnice pentru a permite sectorului securității cibernetice să obțină progrese tehnologice majore și să stăpânească tehnologiile-cheie ale viitorului în materie de securitate cibernetică. În acest context, dezvoltarea de software cu sursă deschisă și de standarde deschise poate contribui la stimularea încrederii, a transparenței și a inovării disruptive, și ar trebui, prin urmare, să facă de asemenea parte din investițiile făcute în cadrul acestui parteneriat public-privat contractual.

Activitatea desfășurată în cadrul parteneriatului public-privat contractual privind securitatea cibernetică va beneficia, de asemenea, de sinergiile cu alte proiecte europene, în special în cazul în care acestea abordează aspecte legate de securitate. Printre acestea se numără parteneriatele public-privat „Fabricile viitorului”, „Clădirile eficiente din punct de vedere energetic”, „5G și volumele mari de date”[36] și alte parteneriate public-privat sectoriale[37],

[36] Parteneriatul public-privat pentru infrastructura 5G & Parteneriatul public-privat pentru valorificarea volumelor mari de date
[37] De exemplu, parteneriatul public-privat SESAR sau „Shift to Rail”.

precum și inițiativa „Internetul obiectelor”[38]. În plus, va fi promovată o aliniere strânsă cu cloudul european destinat științei deschise (*European Open Science Cloud*) și cu inițiativa europeană de calcul intensiv pentru tehnologiile cibernetice cuantice (*European supercomputing initiative for quantum cyber technologies*) (de exemplu, inovarea în domeniul distribuției cuantice a cheilor, cercetarea în domeniul calculului cuantic).

Parteneriatul public-privat contractual privind securitatea cibernetică este lansat în cadrul programului Orizont 2020[39], programul-cadru pentru cercetare și inovare al UE pentru perioada 2014-2020. Acesta va mobiliza fonduri din două componente ale programului: „Poziția de lider în domeniul tehnologiilor generice și industriale” (LEIT-ICT) și provocarea societală „Societăți sigure” (SC7). Bugetul total al PPPc va fi de până la 450 de milioane EUR, cu un triplu efect de levier asupra părții reprezentate de industrie. Securitatea cibernetică ar trebui, de asemenea, să fie abordată și coordonată cu alte părți relevante ale programului Orizont 2020 (de exemplu, provocările societale în sectoarele energiei, transporturilor și al sănătății și componenta „Excelență” din cadrul programului Orizont 2020). Aceste măsuri vor contribui la realizarea obiectivelor parteneriatului public-privat contractual privind securitatea cibernetică. Coordonarea ar trebui, de asemenea, să aibă loc în prealabil, în etapa de definire a strategiilor sectoriale.

PPPc va fi pus în aplicare în mod transparent, în condiții de guvernanță deschisă și flexibilă, adaptată la un mediu de securitate cibernetică în evoluție rapidă. Comisia va lua în considerare necesitatea ca statele membre să discute modul în care schimbările tehnologice afectează funcționarea sigură a infrastructurilor naționale și transfrontaliere. De asemenea, rezultatele parteneriatului trebuie să fie sustenabile pe parcursul mai multor ani pentru a se asigura că obiectivele acestuia pot fi îndeplinite.

PPPc va fi sprijinit de Organizația Europeană pentru Securitate Cibernetică (ECSO - *European Cyber Security Organisation*), a cărei componență va reflecta diversitatea pieței de securitate cibernetică din Europa. Aceasta va include, de asemenea, administrații publice naționale, regionale și locale, centre de cercetare, universități și alte părți interesate.

Comisia:

- va semna cu industria un parteneriat public-privat contractual privind securitatea cibernetică, astfel încât acesta să devină operațional în cel de-al treilea trimestru al anului 2016;
- va lansa cererile de propuneri pentru Orizont 2020 legate de parteneriatul public-privat contractual privind securitatea cibernetică în primul trimestru al anului 2017 și
- va asigura coordonarea parteneriatului public-privat contractual privind securitatea cibernetică cu strategiile sectoriale relevante, cu instrumentele din programul-cadru Orizont 2020 și cu parteneriatele public-privat sectoriale.

[38] Alianța pentru inovare în domeniul internetului obiectelor (*Alliance for Internet of Things Innovation* – AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

5. CONCLUZII

Prezenta comunicare prezintă măsuri menite să consolideze sistemul de reziliență cibernetică al Europei și să promoveze un sector al securității cibernetice competitiv și inovator în Europa, astfel cum s-a anunțat în Strategia de securitate cibernetică a UE și în Strategia privind piața unică digitală. Comisia invită Parlamentul European și Consiliul să susțină această abordare.