COMISIA EUROPEANĂ

ÎNALTUL REPREZENTANT AL UNIUNII EUROPENE PENTRU AFACERI EXTERNE ȘI POLITICA DE SECURITATE

Bruxelles, 7.2.2013
JOIN(2013) 1 final

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Strategia de securitate cibernetică a Uniunii Europene:

un spațiu cibernetic deschis, sigur și securizat

COMUNICARE COMUNĂ CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Strategia de securitate cibernetică a Uniunii Europene:

un spațiu cibernetic deschis, sigur și securizat

1. INTRODUCERE

1.1. Context

În ultimele două decenii, internetul și, într-un sens mai larg, spațiul cibernetic au avut un impact enorm asupra tuturor componentelor societății. Viața noastră de zi cu zi, drepturile noastre fundamentale, interacțiunile sociale și economiile noastre depind de funcționarea neîntreruptă a tehnologiei informației și comunicațiilor. Existența unui spațiu cibernetic deschis și liber a promovat incluziunea politică și socială la nivel mondial. Ea a dărâmat barierele dintre țări, comunități și cetățeni, permițând interacțiunea și schimbul de informații și idei în întreaga lume; a constituit un forum al libertății de exprimare și al exercitării drepturilor fundamentale și a sprijinit oamenii în eforturile lor de a crea societăți democratice și mai drepte – exemplul cel mai grăitor fiind Primăvara arabă.

Pentru ca spațiul cibernetic să rămână deschis și liber, aceleași norme, principii și valori pe care Uniunea Europeană le susține offline ar trebui să se aplice și online. Drepturile fundamentale, democrația și statul de drept au nevoie de protecție în spațiul cibernetic. Libertatea și prosperitatea noastră depind din ce în ce mai mult de un internet robust și inovator, iar acesta va continua să se dezvolte dacă inovațiile din sectorul privat și societatea civilă îi vor sprijini creșterea. Libertatea online presupune însă deopotrivă siguranță și securitate. Spațiul cibernetic ar trebui să fie protejat de incidente, activități rău intenționate și utilizare abuzivă. Administrațiile naționale joacă un rol semnificativ în asigurarea unui spațiu cibernetic liber și sigur. Ele au mai multe sarcini: să salvgardeze accesul și deschiderea, să respecte și să protejeze drepturile fundamentale online și să mențină fiabilitatea și interoperabilitatea internetului. Sectorul privat deține și exploatează însă o parte semnificativă a spațiului cibernetic și, prin urmare, orice inițiativă care dorește să aibă succes în domeniu trebuie să recunoască rolul central jucat de acesta.

Tehnologia informației și comunicațiilor (TIC) a devenit coloana vertebrală a creșterii noastre economice și reprezintă o resursă de importanță majoră pe care se bazează toate sectoarele economiei. TIC stă în prezent la baza sistemelor complexe care asigură funcționarea economiilor noastre, în sectoare-cheie cum ar fi finanțele, sănătatea, energia și transporturile, în timp ce multe modele comerciale sunt construite pornind de la premiza disponibilității neîntrerupte a internetului și a bunei funcționări a sistemelor informatice.

Prin definitivarea pieței unice digitale, Europa și-ar putea mări PIB-ul cu aproximativ 500 de miliarde de euro pe an[1], ceea ce ar însemna, în medie, 1 000 de euro per persoană. Pentru ca noile tehnologii conexe să ia avânt (este vorba, printre altele, de plățile electronice, cloud computing sau comunicarea „de la mașină la mașină”[2]), cetățenii vor trebui să aibă încredere,

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] De exemplu, plante cu senzori integrați care au posibilitatea de a semnala sistemului de aspersoare momentul când trebuie să fie udate.

atât în tehnologiile în sine, cât și în propria capacitate de a le utiliza. Din păcate, un sondaj Eurobarometru din 2012[3] a arătat că aproape o treime dintre europeni nu au încredere în capacitatea lor de a folosi internetul pentru operațiuni bancare sau cumpărături. O majoritate covârșitoare a declarat de asemenea că evită să divulge informații personale online din cauza preocupărilor legate de securitate. La nivelul UE, mai mult de unul din zece utilizatori ai internetului a devenit deja victimă a fraudei online.

În ultimii ani s-a constatat că lumea digitală aduce beneficii enorme, însă ea este în același timp vulnerabilă. Numărul incidentelor de securitate cibernetică[4], fie ele intenționate sau accidentale, crește într-un ritm alarmant și ar putea perturba furnizarea unor servicii esențiale a căror existență o considerăm de la sine-înțeleasă, și anume aprovizionarea cu apă sau energie electrică, asistența medicală sau serviciile de telefonie mobilă. Amenințările pot veni din surse diverse – cum ar fi atacurile criminale, teroriste, motivate politic sau comanditate de stat, precum și catastrofele naturale sau greșelile neintenționate.

Economia UE este deja afectată de actele de criminalitate cibernetică[5] îndreptate împotriva sectorului privat și a persoanelor fizice. Infractorii cibernetici utilizează metode din ce în ce mai sofisticate pentru a pătrunde în sistemele informatice, furând date critice sau cerând răscumpărări întreprinderilor. Dezvoltarea, în spațiul cibernetic, a spionajului economic și a activităților comanditate de stat reprezintă o nouă categorie de amenințări la adresa administrațiilor naționale și a întreprinderilor din UE.

În țări din afara UE, administrațiile naționale pot utiliza abuziv spațiul cibernetic și pentru supravegherea și controlul propriilor cetățeni. UE poate contracara această situație prin promovarea libertății online și asigurarea respectului drepturilor fundamentale online.

Toți acești factori explică motivul pentru care administrațiile naționale din întreaga lume au început să dezvolte strategii în materie de securitate cibernetică și să considere spațiul cibernetic o preocupare internațională din ce în ce mai importantă. A sosit momentul ca UE să își intensifice acțiunile în acest domeniu. Prezenta propunere de strategie de securitate cibernetică a Uniunii Europene, prezentată de Comisie și de Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (denumit în continuare „Înaltul Reprezentant”), prezintă viziunea UE în acest domeniu, clarifică roluri și responsabilități și stabilește acțiunile necesare, pe baza unei protecții și promovări solide și eficace a drepturilor cetățenilor, astfel încât mediul online al UE să devină cel mai sigur din lume.

1.2. Principii ale securității cibernetice

Internetul fără frontiere și multistratificat a devenit unul dintre cele mai puternice motoare ale progresului la nivel mondial, fără vreo supraveghere sau reglementare din partea autorităților naționale. Sectorul privat ar trebui să continue să joace un rol central în construirea și

---

[3] Eurobarometrul special nr. 390 din 2012 referitor la securitatea cibernetică.

[4] Securitatea cibernetică se referă în general la măsurile de salvgardare și acțiunile care pot fi întreprinse pentru a proteja spațiul cibernetic, atât în domeniul civil, cât și în cel militar, de acele amenințări care sunt asociate rețelelor sale interdependente și infrastructurii sale informatice sau sunt susceptibile de a le afecta. Securitatea cibernetică are drept obiectiv să conserve disponibilitatea și integritatea rețelelor și a infrastructurii, precum și confidențialitatea informațiilor conținute de acestea.

[5] Criminalitatea cibernetică se referă în general la o gamă largă de activități infracționale, care au ca instrument principal ori ca țintă principală calculatoarele și sistemele informatice. Criminalitatea cibernetică include infracțiunile tradiționale (de exemplu frauda, falsificarea și furtul de identitate), infracțiunile legate de conținut (de exemplu, distribuirea de pornografie infantilă sau instigarea la ură rasială online) și infracțiunile asociate exclusiv calculatoarelor și sistemelor informatice (de exemplu, atacurile împotriva sistemelor informatice, blocarea accesului și malware-ul).

gestionarea zilnică a internetului, iar necesitatea unor cerințe în materie de transparență, responsabilitate și securitate devine din ce în ce mai acută. Această strategie clarifică principiile care ar trebui să ghideze politica securității cibernetice în UE și la nivel internațional.

Valorile fundamentale ale UE se aplică atât în lumea digitală ca și în cea materială

Aceleași legi și norme care se aplică celorlalte domenii ale vieții noastre de zi cu zi se aplică și domeniului cibernetic.

Protejarea drepturilor fundamentale, a libertății de exprimare, a datelor cu caracter personal și a vieții private

Nu putem beneficia de o securitate cibernetică solidă și eficace decât dacă aceasta se bazează pe drepturile și libertățile fundamentale consacrate prin Carta drepturilor fundamentale a Uniunii Europene și prin valorile fundamentale ale UE. Pe de altă parte, drepturile cetățenilor nu pot fi garantate în absența unor rețele și a unor sisteme sigure. Orice schimb de informații în sensul securității cibernetice, atunci când sunt în joc date cu caracter personal, ar trebui să se desfășoare în conformitate cu legislația UE privind protecția datelor și să respecte îndeaproape drepturile cetățenilor în domeniu.

Acces pentru toți

Accesul limitat sau inexistent la internet și „analfabetismul" digital constituie un dezavantaj pentru cetățeni, având în vedere amprenta marcată a lumii digitale asupra activităților societății. Toată lumea ar trebui să poată avea acces la internet și la un flux neîntrerupt de informații. Integritatea și securitatea internetului trebuie să fie garantate pentru a permite un acces sigur pentru toți.

Guvernanță participativă, democratică și eficientă

Lumea digitală nu este controlată de o singură entitate. Există în prezent o multitudine de părți interesate – dintre care multe sunt entități comerciale și neguvernamentale – implicate atât în gestionarea curentă a resurselor, protocoalelor și standardelor internetului, cât și în dezvoltarea viitoare a acestuia. UE reafirmă importanța rolului jucat de toate părțile interesate în cadrul modelului actual de guvernanță a internetului și sprijină această abordare de guvernanță participativă[6].

O responsabilitate comună pentru asigurarea securității

Dependența din ce în ce mai ridicată de tehnologiile informației și comunicațiilor în toate domeniile vieții omenești a condus la vulnerabilități care trebuie să fie definite în mod corespunzător, analizate temeinic, corectate sau reduse. Toți actorii implicați, fie că este vorba despre autorități publice, sectorul privat sau cetățeni, trebuie să conștientizeze această responsabilitate comună, să ia măsuri pentru a se proteja și, dacă este necesar, să ofere un răspuns coordonat pentru consolidarea securității cibernetice.

[6] A se vedea și COM(2009) 277 - Comunicare a Comisiei către Parlamentul European și Consiliu privind „Guvernarea internetului: etapele următoare".

2. PRIORITĂȚI ȘI ACȚIUNI STRATEGICE

UE ar trebui să salvgardeze un mediu online care oferă cel mai înalt nivel posibil de libertate și securitate, în beneficiul tuturor. Recunoscând faptul că abordarea provocărilor de securitate din spațiul cibernetic cade în principal în sarcina statelor membre, strategia de față propune acțiuni specifice care pot îmbunătăți performanța globală a UE. Aceste acțiuni sunt planificate atât pe termen scurt, cât și pe termen lung. Ele includ o serie de instrumente de politică[7] și implică diferiți actori, de la instituții UE, la state membre și industria de profil.

Viziunea UE, prezentată în această strategie, se articulează pe cinci priorități strategice care abordează provocările menționate mai sus:

- realizarea rezilienței cibernetice;
- reducerea drastică a criminalității cibernetice;
- dezvoltarea politicii și a capacităților de apărare cibernetică legate de politica de securitate și apărare comună (PSAC)
- dezvoltarea resurselor industriale și tehnologice în materie de securitate cibernetică;
- instituirea unei politici internaționale coerente a Uniunii Europene privind spațiul cibernetic și promovarea valorilor fundamentale al UE.

2.1. Realizarea rezilienței cibernetice

Pentru a promova reziliența cibernetică în UE, atât autoritățile publice cât și sectorul privat trebuie să-și dezvolte capacitățile și să coopereze în mod eficient. Pornind de la rezultatele pozitive obținute prin activitățile desfășurate până în prezent[8], continuarea acțiunii la nivelul UE poate ajuta în special la combaterea riscurilor și a amenințărilor cibernetice cu dimensiune transfrontalieră, contribuind la articularea unui răspuns coordonat în situații de urgență. Aceasta va reprezenta un sprijin puternic pentru buna funcționare a pieței interne și va spori securitatea internă a UE.

Europa va rămâne vulnerabilă dacă nu se depun eforturi substanțiale de sporire a capacităților, resurselor și proceselor publice și private destinate a preveni, detecta și gestiona incidentele de securitate cibernetică. Iată de ce Comisia a elaborat o politică privind securitatea rețelelor și a informațiilor (*Network and Information Security* – NIS)[9]. **Agenția Europeană pentru Securitatea Rețelelor și a Informațiilor** (*European Network and Information Security Agency***,** ENISA) a fost înființată în 2004[10] iar, în prezent, Consiliul și Parlamentul negociază un nou regulament vizând consolidarea ENISA și modernizarea mandatului acesteia[11]. În plus, Directiva-cadru privind comunicațiile electronice[12] impune furnizorilor de comunicații

---

7 Acțiunile legate de schimbul de informații, atunci când sunt în joc date cu caracter personal, ar trebui să respecte legislația UE privind protecția datelor.

8 A se vedea referințele din prezenta comunicare, precum și cele din documentul de lucru al serviciilor Comisiei, evaluarea impactului care însoțește propunerea de directivă a Comisiei privind securitatea rețelelor și a informațiilor, în special secțiunile 4.1.4, 5.2 și anexele 2, 6 și 8.

9 În 2001, Comisia a adoptat o comunicare privind „Securitatea rețelelor și a informației: Propunere privind o abordare politică europeană" [COM(2001) 298]; în 2006, ea a adoptat o Strategie pentru o societate informațională securizată [COM(2006) 251]. Din 2009, Comisia a adoptat de asemenea un plan de acțiune și o Comunicare privind protecția infrastructurilor critice de informație (*Critical Information Infrastructure Protection*, CIIP) [COM(2009) 149, confirmată prin Rezoluția 2009/C 321/01 a Consiliului și COM(2011) 163, confirmată prin Concluziile 10299/11 ale Consiliului].

10 Regulamentul (CE) nr. 460/2004.

11 COM(2010) 521. Acțiunile propuse în această strategie nu implică modificarea prezentului sau viitorului mandat al ENISA.

12 Articolul 13 literele (a) și (b) din Directiva 2002/21/CE.

electronice să gestioneze în mod corespunzător riscurile la adresa propriilor rețele și să raporteze atacurile grave la adresa securității. În același timp, legislația UE privind protecția datelor[13] impune operatorilor de date să garanteze respectarea cerințelor și a garanțiilor în materie de protecție a datelor, inclusiv a măsurilor legate de securitate, iar în domeniul serviciilor de comunicații electronice accesibile publicului, operatorii de date trebuie să notifice autorităților naționale competente incidentele care implică violări ale datelor personale.

În ciuda progreselor făcute pe bază de angajamente voluntare, există încă deficiențe în întreaga UE, în special în ceea ce privește capacitățile naționale, coordonarea în caz de incidente cu amploare transfrontalieră și implicarea și pregătirea sectorului privat. Prezenta strategie este însoțită de o propunere **legislativă** vizând, în special:

- stabilirea unor cerințe minime comune în materie de securitate a rețelelor și informației (*Network and Information Security*, NIS) la nivel național, care ar obliga statele membre: să desemneze autorități naționale competente în materie de NIS; să înființeze o echipă CERT performantă și să adopte o strategie și un plan de cooperare naționale în domeniul NIS. Consolidarea și coordonarea capacităților privesc de asemenea și instituțiile UE: în 2012 a fost înființată, cu titlu permanent, o echipă de răspuns în caz de urgențe informatice responsabilă pentru securitatea sistemelor informatice ale instituțiilor, agențiilor și organismelor UE („CERT-UE”);
- instaurarea unor mecanisme coordonate de prevenire, detectare, atenuare și răspuns care să permită schimbul de informații și asistența reciprocă între autoritățile naționale competente în materie de securitate a rețelelor și informației. Autoritățile naționale competente în domeniul NIS vor fi invitate să asigure o cooperarea adecvată la nivelul UE, în special pe baza unui plan de cooperare în acest domeniu la nivelul Uniunii, menit să asigure un răspuns la incidentele cibernetice cu dimensiune transfrontalieră. Această cooperare se va întemeia și pe progresele înregistrate în contextul „Forumului european al statelor membre (FESM)”[14], care a organizat discuții și schimburi de idei fructuoase referitoare la politica publică în domeniul NIS și care poate fi integrat în mecanismul de cooperare, odată ce acesta a fost pus în practică;
- îmbunătățirea pregătirii și a implicării sectorului privat. Deoarece marea majoritate a rețelelor și sistemelor informatice se află în proprietate privată, îmbunătățirea cooperării cu sectorul privat este esențială pentru promovarea securității cibernetice. La nivel tehnic, sectorul privat ar trebui să-și dezvolte propriile capacități de reziliență cibernetică și să facă schimb de bune practici cu celelalte domenii de activitate. Sectorul public ar trebui să poată beneficia și el de instrumentele dezvoltate de industrie pentru intervenția în caz de incident, stabilirea cauzelor și desfășurarea investigațiilor criminalistice.

Actorii privați nu beneficiază încă de stimulente eficiente care să-i încurajeze să furnizeze date fiabile privind existența sau impactul incidentelor de NIS, să adopte o cultură a gestionării riscului sau să investească în soluții de securitate. Legislația propusă vizează, prin urmare, garantarea faptului că actorii dintr-o serie de domenii-cheie (cum ar fi energia, transporturile, serviciile bancare, bursele și facilitatorii de servicii-cheie de internet, precum și administrațiile publice) evaluează riscurile cu care se confruntă în materie de securitate cibernetică, asigură viabilitatea și reziliența rețelelor și a sistemelor informatice prin gestionarea adecvată a riscurilor identificate și fac schimb de informații cu autoritățile

[13] Articolul 17 din Directiva 95/46/CE; Articolul 4 din Directiva 2002/58/CE.

[14] Forumul european al statelor membre a fost lansat prin intermediul COM(2009) 149 ca platformă de promovare a dialogului între autoritățile publice ale statelor membre pe marginea bunelor practici de politică în domeniul securității și rezilienței infrastructurilor critice de informație.

naționale competente în domeniul NIS. Adoptarea unei culturi a securității cibernetice ar putea spori oportunitățile de afaceri și competitivitatea din sectorul privat, fapt ce ar putea transforma securitatea cibernetică într-un atu comercial.

Aceste entități ar trebui să raporteze autorităților naționale competente în domeniul NIS incidentele cu impact semnificativ asupra continuității serviciilor esențiale și a furnizării de mărfuri care depind de rețelele și sistemele informatice.

Autoritățile naționale competente în domeniul NIS ar trebui să colaboreze și să facă schimb de informații cu alte organisme de reglementare și în special cu autoritățile de protecție a datelor cu caracter personal. La rândul lor, autoritățile competente în domeniul NIS ar trebui să raporteze autorităților responsabile cu aplicarea legii incidentele suspectate a fi de natură infracțională gravă. Autoritățile naționale competente ar trebui de asemenea să publice periodic, pe un site web dedicat, informații neconfidențiale referitoare la alertele rapide în curs privind incidente și riscuri, precum și referitoare la răspunsurile coordonate. Obligațiile legale nu ar trebui nici să înlocuiască, nici să împiedice dezvoltarea unei cooperări neoficiale și voluntare, inclusiv între sectorul public și cel privat, în scopul creșterii nivelului de securitate și al schimbului de informații și de bune practici. Parteneriatul public-privat european pentru reziliență (EP3R[15]) este o platformă solidă și valabilă la nivelul UE și ar trebui dezvoltată în continuare.

Facilitatea „Conectarea Europei" (*Connecting Europe Facility*, CEF)[16] ar urma să ofere sprijin financiar infrastructurilor-cheie, conectând capacitățile statelor membre în domeniul NIS pentru facilitarea cooperării la nivelul întregii UE.

În fine, simulările de incidente cibernetice la nivelul UE sunt esențiale pentru a stimula cooperarea dintre statele membre și sectorul privat. Prima simulare de acest fel, care a implicat statele membre, a fost efectuată în 2010, intitulându-se „Cyber Europe 2010". O a doua simulare, implicând și sectorul privat, a avut loc în octombrie 2012 sub denumirea „Cyber Europe 2012". Sub titulatura „Cyber Atlantic 2011" în noiembrie 2011 a avut loc o simulare pe calculator între UE-SUA, alte simulări fiind prevăzute pentru anii următori, inclusiv cu parteneri internaționali.

Comisia intenționează:

- să-și continue activitățile, desfășurate de Centrul Comun de Cercetare în strânsă coordonare cu autoritățile statelor membre și cu proprietarii și operatorii de infrastructuri critice, ce au ca scop identificarea vulnerabilităților în materie de NIS ale infrastructurilor critice europene și încurajarea dezvoltării unor sisteme reziliente.
- să lanseze, la începutul anului 2013, un proiect-pilot finanțat de UE[17] vizând **combaterea botneturilor și a malware-ului**, pentru a oferi un cadru de

15 Parteneriatului public-privat european pentru reziliență a fost lansat prin intermediul COM(2009) 149. Această platformă a inițiat lucrări și a încurajat cooperarea dintre sectorul public și cel privat în ceea ce privește identificarea principalelor active, resurse, funcții și cerințe de bază în materie de reziliență, a nevoilor de cooperare și a mecanismelor de intervenție în caz de perturbări majore ale comunicațiilor electronice.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Linia bugetară CEF 09.03.02 – Rețele de telecomunicații (pentru promovarea interconectării și a interoperabilității serviciilor publice online naționale, precum și accesul la aceste rețele).

coordonare și cooperare între statele membre ale UE, organizațiile din sectorul privat - cum ar fi furnizorii de servicii de internet și parteneri internaționali.

Comisia invită ENISA:

- să sprijine statele membre în dezvoltarea unor puternice **capacități naționale de reziliență cibernetică**, în special prin dobândirea de competențe în materie de securitate și reziliență a sistemelor industriale de control și a infrastructurii transporturilor și energiei;
- să examineze, în 2013, fezabilitatea echipei sau a echipelor de răspuns la incidente de securitate cibernetică pentru sistemele de control industrial (*Computer Security Incident Response Team for Industrial Control Systems*, ICS-CSIRT) pentru UE.
- să continue sprijinirea statelor membre și a instituțiilor UE în efectuarea de **simulări** periodice **ale unor incidente cibernetice paneuropene** care vor constitui totodată baza operațională a participării UE la simulările internaționale de incidente cibernetice.

Comisia invită Parlamentul European și Consiliul:

- **să adopte** rapid propunerea de directivă privind **un nivel comun ridicat de securitate a rețelelor și a informației (NIS)** în întreaga Uniune, abordând chestiuni precum capacitățile și pregătirea la nivelul statelor membre, cooperarea la nivelul UE, adoptarea practicilor de gestionare a riscului și schimbul de informații în domeniul NIS.

Comisia invită industria de profil:

- să devină lideri în ceea ce privește investițiile într-un nivel ridicat de securitate cibernetică și să dezvolte bunele practici și schimbul de informații la nivel de sector și cu autoritățile publice, pentru a asigura o protecție puternică și eficientă a bunurilor și a persoanelor, în special prin intermediul unor parteneriate public-privat precum EP3R și *Trust in Digital Life* (Încrederea în viața digitală), TDL[18].
-

Sensibilizare

Asigurarea securității cibernetice este o responsabilitate comună. Utilizatorii finali joacă un rol esențial în asigurarea securității rețelelor și a sistemelor informatice: ei trebuie să fie informați cu privire la riscurile cu care se confruntă online și abilitați să ia măsuri simple de protecție împotriva acestora.

În ultimii ani au fost dezvoltate o serie de inițiative care trebuie continuate. Mai exact, ENISA a fost implicată în acțiuni de sensibilizare prin publicarea de rapoarte, organizarea de ateliere ale experților și dezvoltarea de parteneriate public-privat. Europol, Eurojust și autoritățile naționale de protecție a datelor desfășoară, de asemenea, acțiuni de sensibilizare a opiniei publice. Împreună cu unele state membre, ENISA a coordonat, în octombrie 2012, „Luna europeană a securității cibernetice". Sensibilizarea reprezintă unul dintre domeniile promovate de Grupul de lucru UE-SUA pe

[17] CIP-ICT PSP-2012-6, 325188 (PSP TIC din cadrul PCCI, 6-2012, nr. 325188). Programul are un buget total de 15 milioane de euro, din care 7,7 milioane de euro reprezintă finanțare de la bugetul UE.

[18] http://www.trustindigitallife.eu/

probleme de securitate și criminalitate cibernetică[19] și este, de asemenea, esențială în contextul Programului pentru un internet mai sigur[20], axat pe siguranța copiilor online.

Comisia invită ENISA:

- să propună, în 2013, o foaie de parcurs pentru un „permis de conducere” în domeniul securității rețelelor și a informației, sub forma unui program de certificare voluntară care să promoveze aptitudini și competențe sporite ale profesioniștilor domeniului TI (de exemplu, administratorii de site-uri web).

Comisia intenționează:

- să organizeze, în 2014, cu sprijinul ENISA, un **campionat** al securității cibernetice adresat studenților, unde aceștia vor participa cu propuneri de soluții în domeniul NIS.

Comisia invită statele membre[21]:

- să organizeze în fiecare an – cu sprijinul ENISA și, începând din 2013, cu implicarea sectorului privat – o **lună a securității cibernetice**, având ca obiectiv sensibilizarea utilizatorilor finali. Începând din 2014, se va organiza o lună a securității cibernetice, în mod sincronizat în UE și în SUA.
- **să-și intensifice eforturile la nivel național în ceea ce privește educarea și formarea în domeniul NIS**, prin introducerea: formării în domeniul NIS în școli, până în 2014; formării în domeniile NIS, al dezvoltării de software securizat și al protecției datelor personale pentru studenții facultăților de informatică; și a formării de bază în domeniul NIS pentru personalul al administrațiilor publice.

Comisia invită industria de profil:

- să promoveze **sensibilizarea** în materie de securitate cibernetică **la toate nivelurile**, atât în practicile comerciale, cât și în relația cu clienții. Mai exact, întreprinderile ar trebui să reflecteze asupra modalităților de a face astfel încât responsabilitatea asigurării securității cibernetice să revină într-o mai mare măsură directorilor și consiliilor de administrație.

2.2. Reducerea drastică a criminalității cibernetice

Cu cât petrecem mai mult timp în lumea digitală, cu atât oferim mai multe oportunități infractorilor cibernetici. Criminalitatea cibernetică este o formă de criminalitate cu una dintre cele mai rapide rate de creștere, ei căzându-i victime în întreaga lume peste un milion de persoane în fiecare zi. Infractorii cibernetici și rețelele criminalității cibernetice devin din ce

[19] Acest grup de lucru, constituit în cadrul întâlnirii la nivel înalt UE-SUA din noiembrie 2010 (MEMO/10/597), este însărcinat cu elaborarea unor abordări colaborative în ceea ce privește o gamă largă de aspecte referitoare la securitatea și criminalitatea cibernetică.

[20] Programul pentru un internet mai sigur finanțează o rețea de ONG-uri active în domeniul protecției copilului online, o rețea de organisme de aplicare a legii care schimbă informații și bune practici legate de exploatarea ilicită a internetului prin difuzarea de materiale conținând abuzuri sexuale comise asupra copiilor și o rețea de cercetători care culeg informații despre utilizarea, riscurile și consecințele tehnologiilor online în ceea ce privește viețile copiilor.

[21] Cu participarea autorităților naționale implicate, inclusiv a autorităților competente în domeniul NIS și a autorităților de protecție a datelor.

în ce mai sofisticate și trebuie să dispunem de instrumentele operaționale și capacitățile adecvate pentru a le aborda. Infracțiunile cibernetice sunt activități cu profit ridicat și cu risc scăzut, infractorii exploatând deseori anonimatul domeniilor web. Criminalitatea cibernetică nu cunoaște granițe – întinderea mondială a internetului însemnând că organismele de aplicare a legii trebuie să adopte o abordare transfrontalieră coordonată și colaborativă pentru a răspunde acestei amenințări în creștere.

O legislație solidă și eficientă

UE și statele membre au nevoie de o legislație solidă și eficientă pentru a combate criminalitatea cibernetică. Convenția Consiliului Europei privind criminalitatea cibernetică, cunoscută și sub denumirea Convenția de la Budapesta, este un tratat internațional obligatoriu care oferă un cadru eficient pentru adoptarea legislației naționale.

UE a adoptat deja o legislație în materie de criminalitate cibernetică, inclusiv o directivă privind combaterea exploatării sexuale online a copiilor și a pornografiei infantile[22]. De asemenea, UE este pe punctul de a ajunge la un acord referitor la o directivă privind atacurile împotriva sistemelor informatice, în special prin utilizarea botneturilor.

Comisia intenționează:

- să asigure transpunerea și punerea în aplicare rapidă a directivelor privind criminalitatea cibernetică.
- să îndemne cu tărie statele membre care nu au ratificat până în prezent **Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică** să ratifice și să pună în aplicare cât mai curând posibil dispozițiile acesteia.

Capacitate operațională sporită de a combate criminalitatea cibernetică

Tehnicile în materie de criminalitate cibernetică au evoluat rapid, iar organismele de aplicare a legii nu pot combate criminalitatea cibernetică utilizând instrumente operaționale perimate. În prezent, nu toate statele membre ale UE au capacitatea operațională de care au nevoie pentru a răspunde în mod eficient criminalității cibernetice. Toate statele membre au nevoie de unități naționale eficiente de combatere a criminalității cibernetice.

Comisia intenționează:

- să sprijine statele membre, prin intermediul programelor sale de finanțare[23], în eforturile acestora de **a identifica lacunele și** de **a-și consolida capacitatea** de investigare și combatere a criminalității cibernetice. În plus, Comisia va sprijini organismele care fac legătura între de cercetători/mediile universitare, profesioniști din domeniul aplicării legii și sectorul privat, similar cu activitatea desfășurată în prezent de Centrele de excelență pentru combaterea criminalității cibernetice, finanțate de Comisie și instituite deja în unele state membre.
- împreună cu statele membre și cu sprijinul JRC, să coordoneze eforturile în

[22] Directiva 2011/92/UE a Consiliului de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului.

[23] Pentru 2013, în cadrul Programului de prevenire și combatere a criminalității (ISEC). După 2013, în cadrul Fondului pentru securitate internă (nou instrument în cadrul CFM).

vederea identificării celor mai bune practici și tehnici disponibile de luptă împotriva criminalității cibernetice (de exemplu, în ceea ce privește dezvoltarea și utilizarea unor instrumente de expertiză criminalistică sau pentru analizarea amenințărilor)

- să colaboreze îndeaproape cu **Centrul european de combatere a criminalității informatice** (*European Cybercrime Centre*, EC3), recent creat **în cadrul Europol și cu Eurojust** în vederea alinierii acestor abordări politice cu cele mai bune practici de pe partea operațională.

O coordonare sporită la nivelul UE

UE poate completa eforturile statelor membre prin facilitarea unei abordări coordonate și colaborative, reunind autorități judiciare și autorități de aplicare a legii, părți interesate din sectorul public și privat din Uniunea Europeană și din afara acesteia.

Comisia intenționează:

- să sprijine recent creatul **Centru european de combatere a criminalității informatice** (EC3) ca punct focal european în domeniu. EC3 va furniza analize și informații, va sprijini anchetele, va furniza un nivel ridicat de expertiză criminalistică, va facilita cooperarea, va crea canale pentru schimbul de informații dintre autoritățile competente din statele membre, sectorul privat și alte părți interesate și, treptat, își va asuma rolul de portavoce al profesioniștilor organismelor de aplicare a legii[24].
- să sprijine eforturile care vizează creșterea responsabilității birourilor de înregistrare a numelor de domenii și asigurarea acurateței informațiilor privind proprietarii site-urilor web, în special pe baza recomandărilor de aplicare a legii privind *Internet Corporation for Assigned Names and Numbers* (ICANN), în conformitate cu dreptul Uniunii, inclusiv cu normele privind protecția datelor.
- bazându-se pe legislația recentă, să continue întărirea eforturilor UE de a combate abuzul sexual online asupra copiilor. Comisia a adoptat o Strategie europeană pentru un internet mai bun pentru copii[25] și, împreună cu state membre și nemembre ale UE, a lansată o Alianță mondială împotriva abuzului sexual online asupra copiilor[26]. Alianța este vectorul unor acțiuni ulterioare ale statelor membre, sprijinite de Comisie și de EC3.

Comisia invită Europol (EC3):

- să-și concentreze inițial sprijinul analitic și operațional asupra anchetelor desfășurate de statele membre în domeniul criminalității cibernetice, pentru a contribui la eliminarea și dezorganizarea rețelelor de criminalitate cibernetică în

[24] La 28 martie 2012, Comisia Europeană a adoptat o comunicare intitulată „Combaterea criminalității în era digitală actuală: instituirea unui Centru european de combatere a criminalității informatice”.

[25] COM(2012) 196 final.

[26] Concluziile Consiliului privind o Alianță mondială împotriva abuzului sexual online asupra copiilor (declarația comună UE-SUA) din 7 și 8 iunie 2012 și Declarația privind lansarea Alianței mondiale împotriva abuzului sexual online asupra copiilor (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

special în domeniile abuzurilor sexuale asupra copiilor, plăților frauduloase, botneturilor și intruziunii;

- să producă periodic rapoarte strategice și operaționale privind tendințele și amenințările emergente cu scopul de a identifica prioritățile și a viza anchetele întreprinse de echipele dedicate combaterii criminalității cibernetice, din statele membre.

Comisia invită Colegiului European de Poliție (CEPOL), în cooperare cu Europol:

- să coordoneze proiectarea și planificarea cursurilor de formare pentru a furniza organismelor de aplicare a legii cunoștințele și competențele necesare pentru a combate în mod eficient criminalitatea cibernetică.

Comisia invită Eurojust:

- să identifice principalele obstacole aflate în calea cooperării judiciare din cadrul anchetelor privind criminalitatea cibernetică și a coordonării dintre statele membre și cu țări terțe și să sprijine anchetarea și urmărirea penală a infracțiunilor cibernetice, atât la nivel operațional, cât și la nivel strategic, precum și activitățile de formare în domeniu.

Comisia invită Eurojust și Europol (EC3):

- să coopereze strâns, de exemplu prin intermediul schimbului de informații, cu scopul de a obține o eficiență sporită în combaterea criminalității cibernetice, conform propriilor mandate și competențe.
-

2.3. Dezvoltarea politicii și a capacităților de apărare cibernetică legate de politica de securitate și apărare comună (PSAC)

Eforturile UE în domeniul securității cibernetice implică și dimensiunea apărării cibernetice. Pentru a spori reziliența sistemelor informatice și de comunicații care sprijină interesele în materie de apărare și securitate națională ale statelor membre, dezvoltarea capacităților de apărare cibernetică ar trebui să se concentreze asupra detectării, reacției și revenirii la starea de normalitate în urma amenințărilor cibernetice sofisticate.

Dat fiind faptul că amenințările îmbracă diferite forme, ar trebui consolidate sinergiile dintre abordările civile și militare în ceea ce privește protejarea activelor cibernetice critice. Aceste eforturi ar trebui sprijinite prin cercetare și dezvoltare și printr-o cooperare mai strânsă între administrațiile naționale, sectorul privat și mediul universitar din UE. Pentru a evita suprapunerile, UE va explora diferite posibilități prin care UE și NATO își pot completa eforturile de mărire a rezilienței infrastructurilor critice de stat, a celor de apărare și a altor infrastructuri informatice de care depind membrii ambelor organizații.

Înaltul Reprezentant se va concentra asupra următoarelor activități-cheie și va invita statele membre și Agenția Europeană de Apărare să colaboreze:

- evaluarea cerințelor operaționale ale UE în materie de apărare cibernetică și promovarea dezvoltării capacităților și tehnologiilor de apărare cibernetică ale UE pentru a aborda toate aspectele legate de dezvoltarea capacității – inclusiv doctrina, competențele manageriale, organizarea, personalul, formarea, tehnologia, infrastructura, logistica și interoperabilitatea;

- dezvoltarea cadrului politic de apărare cibernetică al UE pentru protejarea rețelelor în contextul misiunilor și al operațiunilor PSAC, inclusiv gestionarea dinamică a riscului, îmbunătățirea analizei amenințărilor și a schimbului de informații; îmbunătățirea posibilităților de formare și de participare la exerciții în domeniul apărării cibernetice și context european și multinațional, inclusiv integrarea unor elemente de apărare cibernetică în actualele programe de exerciții militare;

- promovarea dialogului și a coordonării dintre actorii civili și cei militari în UE, punând în special accentul pe schimbul de bune practici, schimbul de informații și alerta rapidă, răspunsul în caz de incidente, evaluarea riscurilor, sensibilizare și stabilirea securității cibernetice ca prioritate;

- asigurarea dialogului cu parteneri internaționali, inclusiv cu NATO, cu alte organizații internaționale și centre de excelență multinaționale, pentru a asigura existența unor capacități reale de apărare, identificarea domeniilor de cooperare și evitarea duplicării eforturilor.

2.4. Dezvoltarea resurselor industriale și tehnologice în materie de securitate cibernetică

Europa dispune de excelente capacități de cercetare și dezvoltare, dar mulți dintre liderii mondiali în furnizarea de produse și servicii inovatoare în domeniul TIC sunt situați în afara UE. Există un risc că Europa să devină extrem de dependentă nu doar de TIC produse în altă parte, dar și de soluții de securitate elaborate în afara frontierelor sale. Este esențial să se garanteze că componentele de hardware și software produse în UE și în țări terțe, care sunt utilizate pentru servicii și infrastructuri critice și din ce în ce mai mult pentru dispozitive mobile sunt demne de încredere și securizate și că ele garantează protecția datelor cu caracter personal.

Promovarea unei piețe unice a produselor din domeniul securității cibernetice

Asigurarea unui nivel ridicat de securitate este posibilă doar dacă toate verigile lanțului valoric (i.e. producătorii de echipamente, dezvoltatorii de software, furnizorii de servicii ai societății informaționale) fac din securitate o prioritate. S-ar părea[27] însă că în opinia multor actori ai pieței, securitatea este mai degrabă o sarcină suplimentară, fapt care se traduce printr-o cerere scăzută de soluții de securitate. Este nevoie de introducerea unor cerințe corespunzătoare de performanță în materie de securitate cibernetică de-a lungul întregului lanț valoric al produselor TIC utilizate în Europa. Sectorul privat trebuie stimulat să asigure un nivel ridicat de securitate cibernetică; de exemplu, existența unor etichete care să indice performanța adecvată în domeniul securității cibernetice va permite întreprinderilor cu o

[27] A se vedea documentul de lucru al serviciilor Comisiei (evaluarea impactului) care însoțește propunerea de directivă a Comisiei privind securitatea rețelelor și a informației, Secțiunea 4.1.5.2.

performanță bună și documentată în materie să transforme această realitate într-un atu comercial și să obțină un avantaj competitiv. De asemenea, obligațiile enunțate în propunerea de directivă privind NIS ar contribui în mod semnificativ la sporirea competitivității întreprinderilor ce activează în sectoarele vizate.

Ar trebui de asemenea stimulată cererea de produse de înaltă securitate pe piața întregii Europe. În primul rând, strategia de față își propune sporirea cooperării și a transparenței în ceea ce privește securitatea produselor TIC. Ea cheamă la instituirea unei platforme care să reunească părți interesate relevante din sectoarele public și privat europene, pentru a identifica bune practici în materie de securitate cibernetică de-a lungul întregului lanț valoric și a crea condiții de piață favorabile dezvoltării și adoptării de soluții TIC securizate. Un prim obiectiv ar trebui să fie crearea unor stimulente vizând asigurarea unei gestionări adecvate a riscurilor și adoptarea de standarde și soluții de securitate, precum și, eventual, crearea unor sisteme de certificare voluntare la nivelul întregii UE, pornind de la sisteme existente în prezent în UE și la nivel internațional. Comisia va promova adoptarea unor abordări coerente în rândul statelor membre pentru a evita disparitățile care cauzează dezavantaje de ordin geografic pentru întreprinderi.

În al doilea rând, Comisia va susține elaborarea standardelor de securitate și va contribui la acest proces prin instituirea la nivelul întregii UE a unor sisteme de certificare voluntare în domeniul cloud-computingului, ținând totodată cont în mod corespunzător de necesitatea de a asigura protecția datelor. Eforturile ar trebui să se concentreze pe securitatea lanțului de aprovizionare, în special în sectoarele economice critice (sistemele de control industrial, infrastructura energetică și cea de transport). Aceste lucrări ar trebui să se bazeze pe activitatea de standardizare desfășurată în prezent de organizațiile europene de standardizare (CEN, CENELEC și ETSI)[28], de Grupul de coordonare a securității cibernetice (*Cybersecurity Coordination Group*, CSCG), precum și pe expertiza ENISA, a Comisiei și a altor actori implicați.

Comisia intenționează:

- să lanseze în 2013 **o platformă** public-privată **a soluțiilor în materie de NIS**, cu scopul elaborării de stimulente pentru adoptarea unor soluții TIC securizate și a unei culturi a bunei performanțe în materie de securitate cibernetică, care să fie aplicate produselor TIC utilizate în Europa;
- ca, pornind de la rezultatele activităților acestei platforme, să propună, în 2014, recomandări vizând asigurarea securității cibernetice de-a lungul întregului lanț valoric al TIC;
- să examineze modul în care furnizorii importanți de hardware și software TIC ar putea informa autoritățile naționale competente în legătură cu acele vulnerabilități constatate care ar putea avea repercusiuni semnificative asupra securității.

Comisia invită ENISA:

- să elaboreze, în cooperare cu autoritățile naționale competente, părțile interesate implicate, organismele europene și internaționale de standardizare și Centrul comun de cercetare al Comisiei Europene **orientări și recomandări tehnice privind adoptarea de standarde și bune practici în materie de NIS** în sectorul

[28] În special în temeiul Standardului pentru rețelele inteligente M/490 pentru primul set de standarde referitor la o rețea inteligentă și o arhitectură de referință.

public și cel privat.

Comisia invită părțile interesate din sectoarele public și privat:

- să stimuleze elaborarea și adoptarea, la inițiativa industriei de sector, a unor **standarde de securitate**, norme tehnice și principii de „securitate prin concepție” și „respect al vieții private prin concepție” de către fabricanții de produse și furnizorii de servicii TIC, inclusiv de către furnizorii de cloud computing; Noile generații de software și hardware ar trebui să fie echipate cu **elemente de securitate mai solide, integrate și ușor de utilizat**.
- să elaboreze, la inițiativa industriei de sector, standarde de performanță în materie de securitate cibernetică destinate întreprinderilor și să amelioreze calitatea informațiilor aflate la dispoziția publicului prin crearea unor **etichete de securitate** sau a unor etichete de calitate care i-ar ajuta consumatorii să „navigheze” pe piață.

Promovarea investițiilor și a inovării în domeniul cercetării și dezvoltării

Cercetarea și dezvoltarea (C&D) are capacitatea de a susține o politică industrială puternică, de a promova o industrie europeană de încredere a TIC, de a impulsiona piața internă și reduce dependența Europei de tehnologii străine. C&D ar trebui să acopere lacunele tehnologice existente în domeniul securității TIC, să anticipeze următoarea generație de provocări în materie de securitate, să țină cont de evoluția constantă a necesităților utilizatorilor și să beneficieze de avantajele tehnologiilor cu dublă utilizare. Aceasta ar trebui totodată să sprijine în continuare dezvoltarea criptografiei. Aceste lucrări trebuie să fie completate de eforturile de a traduce rezultatele C&D în soluții comerciale prin asigurarea stimulentelor necesare și crearea condițiilor de politică adecvate.

UE ar trebui să profite la maximum de Programul-cadru pentru cercetare și inovare Orizont 2020[29], care urmează să fie lansat în 2014. Propunerea Comisiei conține obiective specifice, conforme cu prezenta strategie și care vizează promovarea unor TIC de încredere și combaterea criminalității cibernetice. Orizont 2020 va sprijini cercetarea în materie de securitate a tehnologiilor TIC emergente, va oferi soluții pentru sisteme, servicii și aplicații TIC sigure capăt la capăt, va oferi stimulentele necesare punerii în aplicare și adoptării soluțiilor existente și va aborda interoperabilitatea rețelelor și a sistemelor informatice. La nivelul UE se va acorda o atenție deosebită aspectelor legate de optimizarea și coordonarea diferitelor programe de finanțare (Orizont 2020, Fondul pentru securitate internă, cercetarea din cadrul Agenției Europene de Apărare, inclusiv cooperarea-cadru europeană).

Comisia intenționează:

- să utilizeze programul Orizont 2020 pentru a aborda o gamă de aspecte legate de respectarea vieții private și de securitate în domeniul TIC, de la C&D la inovare și implementare. Orizont 2020 va elabora, de asemenea, unelte și instrumente de combatere a activităților criminale și teroriste care vizează mediul cibernetic.
- să instituie mecanisme pentru o mai bună coordonare a programelor de cercetare

[29] „Orizont 2020” este instrumentul financiar prin care se pune în aplicare inițiativa emblematică a Strategiei Europa 2020 intitulată „O Uniune a inovării”, care își propune să asigure competitivitatea Europei pe plan mondial. Derulat între 2014 și 2020, noul program-cadru al UE pentru cercetare și inovare va fi parte a eforturilor de a crea o nouă creștere și noi locuri de muncă în Europa.

ale instituțiilor Uniunii Europene și ale statelor membre și să stimuleze creșterea investițiilor statelor membre în C&D.

Comisia invită statele membre:

- să dezvolte, până la sfârșitul anului 2013, bune practici în ceea ce privește utilizarea **puterii de cumpărare a administrațiilor publice** (de exemplu prin intermediul achizițiilor publice) pentru a stimula dezvoltarea și implementarea unor elemente de securitate în produsele și serviciile TIC.
- să încurajeze implicarea precoce a industriei de profil și a mediului universitar în dezvoltarea și coordonarea de soluții. Această implicare ar trebui realizată prin utilizarea la maximum a bazei industriale a Europei și a inovațiilor tehnologice asociate provenind din C&D și ar trebui coordonată cu programele de cercetare ale organizațiilor civile și militare.

Comisia invită Europol și ENISA:

- să identifice tendințele și necesitățile emergente ținând cont de evoluția tiparelor criminalității cibernetice și ale securității cibernetice, pentru a dezvolta instrumente și tehnologii digitale de expertiză criminalistică corespunzătoare.

Comisia invită părțile interesate din sectoarele public și privat:

- să dezvolte, în cooperare cu sectorul asigurărilor, **bareme armonizate de calculare a primelor de risc**, care ar permite întreprinderilor care au făcut investiții în securitate să beneficieze de prime de risc mai mici.

2.5. Instituirea unei politici internaționale coerente a Uniunii Europene privind spațiul cibernetic și promovarea valorilor fundamentale al UE

Păstrarea unui spațiu cibernetic deschis, liber și securizat reprezintă o provocare la nivel mondial, pe care UE ar trebui să o abordeze împreună cu partenerii și organizațiile internaționale relevante, sectorul privat și societatea civilă.

În cadrul politicii sale internaționale privind spațiul cibernetic, UE va căuta să promoveze deschiderea și libertatea internetului, să încurajeze eforturile de dezvoltare a unor norme de conduită și să aplice legislația internațională existentă în spațiul cibernetic. UE va lucra, de asemenea, la eliminarea diviziunii digitale și va participa în mod activ la eforturile internaționale de consolidare a capacităților în domeniul securității cibernetice. Implicarea internațională a UE în aspectele cibernetice va fi ghidată de valorile sale fundamentale, și anume demnitatea umană, libertatea, democrația, egalitatea și statul de drept, precum și de respectarea drepturilor fundamentale.

Integrarea chestiunilor legate de spațiul cibernetic în relațiile externe și în politica externă și de securitate comună ale UE

Comisia, Înaltul Reprezentant și statele membre ar trebui să definească o politică internațională coerentă a UE privind spațiul cibernetic, având ca obiectiv adâncirea colaborării și întărirea relațiilor cu principalii parteneri și organizații internaționale, precum și cu societatea civilă și sectorul privat. S-ar impune conceperea, coordonarea și punerea în practică a unor consultări ale UE cu parteneri internaționali referitoare la aspecte cibernetice, pentru a adăuga valoare dialogurilor bilaterale existente între statele membre ale UE și țări terțe. UE va pune un accent reînnoit pe dialogul cu țările terțe, acordând o atenție specială

partenerilor cu viziuni asemănătoare, care împărtășesc valorile UE. Ea va încuraja atingerea unui nivel ridicat de protecție a datelor, inclusiv în ceea ce privește transferul de date personale către o țară terță. Pentru a răspunde provocărilor mondiale legate de spațiul cibernetic, UE va căuta o mai strânsă cooperare cu organizații active în domeniu, cum sunt Consiliul Europei, OCDE, ONU, OSCE, NATO, UA, ASEAN și OAS. La nivel bilateral, cooperarea cu Statele Unite ale Americii este deosebit de importantă și va fi dezvoltată în continuare, în special în contextul Grupului de lucru UE-SUA privind securitatea și criminalitatea cibernetică.

Unul dintre elementele principale ale politicii cibernetice internaționale a UE va fi promovarea spațiul cibernetic ca spațiu al libertății și al drepturilor fundamentale. Lărgirea accesului la internet ar trebui să impulsioneze reforma democratică și să o promoveze la nivel mondial. Creșterea conectivității la nivel mondial nu ar trebui să fie însoțită de cenzură sau de supraveghere în masă. UE ar trebui să promoveze responsabilitatea socială a întreprinderilor[30] și să lanseze inițiative internaționale pentru a spori coordonarea în domeniu la nivel mondial.

Responsabilitatea unui spațiu cibernetic mai securizat revine tuturor participanților la societatea informațională mondială, de la cetățeni la administrațiile naționale. UE sprijină eforturile de definire a unor norme de conduită în spațiul cibernetic, pe care toate părțile interesate ar trebui să le respecte. Așa după cum UE le pretinde cetățenilor săi să respecte drepturile civice, responsabilitățile sociale și legile online, statele ar trebui și ele să respecte norme și legile existente. În ceea ce privește aspectele legate de securitatea internațională, UE încurajează elaborarea unor măsuri de consolidare a încrederii în securitatea cibernetică, pentru a spori transparența și a reduce riscul de interpretare greșită a acțiunilor statului.

UE nu cheamă la crearea de noi instrumente juridice internaționale pentru aspectele cibernetice.

Obligațiile legale consacrate în Pactul internațional privind drepturile civile și politice, Convenția europeană a drepturilor omului și Carta drepturilor fundamentale a Uniunii Europene ar trebui să fie respectate și în mediul online. UE se va concentra asupra modalităților de a garanta aplicarea acestor măsuri și în spațiul cibernetic.

Pentru a aborda problema criminalității cibernetice, Convenția de la Budapesta este un instrument deschis adoptării de către țări terțe. Ea oferă un model pentru redactarea legislației naționale în materie de criminalitatea cibernetică și o bază pentru cooperarea internațională în domeniu.

În situația în care conflictele armate se extind în spațiul cibernetic, se vor aplica dreptul umanitar internațional și, după caz, legea drepturilor omului, în funcție de circumstanțele fiecărui caz în parte. **Consolidarea capacităților în domeniul securității cibernetice și al infrastructurilor informatice reziliente în țări terțe**

Intensificarea cooperării internaționale va avea un impact benefic asupra bunei funcționări a infrastructurilor de bază care furnizează și facilitează servicii de comunicații. Este vorba despre schimbul de bune practici și de informații, despre exerciții de alertă rapidă și gestionare comună a incidentelor etc. UE va contribui la realizarea acestui obiectiv prin intensificarea eforturilor internaționale actuale de întărire a rețelelor de cooperare dintre

[30] O nouă strategie a UE (2011-2014) pentru responsabilitatea socială a întreprinderilor; COM(2011) 681 final.

administrațiile publice și sectorul privat pe probleme de protecție a infrastructurilor critice de informație (CIIP).

Nu toate regiunile lumii beneficiază de pe urma efectelor pozitive ale internetului, din cauza absenței unui acces liber, securizat, interoperabil și fiabil. Uniunea Europeană va continua, prin urmare, să sprijine eforturile depuse de țări în demersul acestora de a oferi propriilor cetățeni un acces la internet pe scară mai largă și în condiții mai bune, de a asigura integritatea și securitatea internetului și de a lupta împotriva criminalității cibernetice.

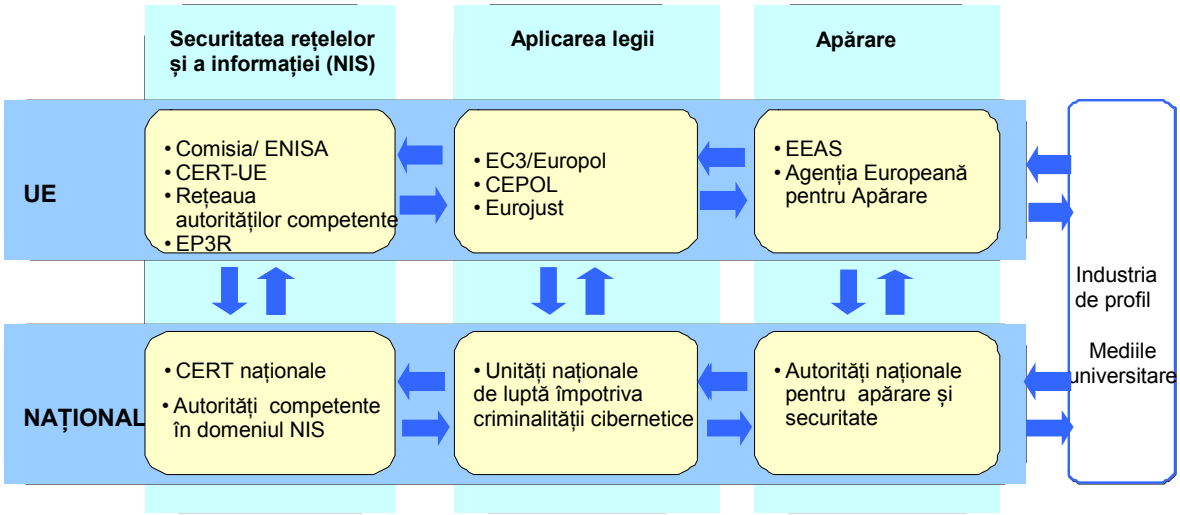
În cooperare cu statele membre, Comisia și Înaltul Reprezentant:

- vor depune eforturi în direcția elaborării unei politici internaționale coerente a UE privind spațiul cibernetic, pentru a adânci colaborarea cu principalii parteneri și organizații internaționale, pentru a integra aspectele cibernetice în PESC și a îmbunătăți coordonarea aspectelor cibernetic de amploare mondială;
- vor sprijini dezvoltarea normelor de conduită și a măsurilor de consolidare a încrederii în securitatea cibernetică. vor facilita dialoguri privind modalitățile de aplicare, în spațiul cibernetic, a legislației internaționale existente și de promovare a Convenția de la Budapesta pentru combaterea criminalității cibernetice;
- vor sprijini promovarea și protecția drepturilor fundamentale, inclusiv accesul la informație și libertatea de exprimare, axându-se pe: a) elaborarea de noi orientări privind libertatea de exprimare online și offline; b) monitorizarea exportului de produse sau servicii care ar putea fi utilizate în scop de cenzură sau de supraveghere în masă online; c) elaborarea de măsuri și instrumente care să permită extinderea accesului la internet, creșterea gradului de deschidere și a rezilienței acestuia pentru a combate supravegherea în masă sau cenzura exercitate prin intermediul tehnologiei comunicațiilor; d) abilitarea părților interesate în ceea ce privește utilizarea tehnologiei comunicațiilor pentru promovarea drepturilor fundamentale;
- vor colabora cu parteneri și organizații internaționale, cu sectorul privat și societatea civilă pentru a sprijini consolidarea capacității la nivel mondial a țărilor terțe de a îmbunătăți accesul la informații și la un internet deschis, de a preveni și a combate amenințările cibernetice, inclusiv evenimentele accidentale, criminalitatea cibernetică și terorismul cibernetic și de a întări coordonarea dintre donatori în scopul canalizării eforturilor de consolidare a capacității;
- vor recurge la diferite instrumente de ajutor UE pentru a consolida capacitatea în materie de securitate cibernetică, inclusiv prin sprijinirea formării personalului organismelor de aplicare a legii, a personalului judiciar și a celui tehnic în scopul combaterii amenințărilor cibernetice și prin sprijinirea creării unor politici naționale, strategii și instituții relevante în țările terțe;
- vor spori coordonarea politicilor și a schimbului de informații prin intermediul rețelelor internaționale de protecție a infrastructurilor critice de informații, cum ar fi rețeaua Meridian, precum și cooperarea dintre și cu autoritățile competente din domeniul NIS și alte organisme.

3. ROLURI ȘI RESPONSABILITĂȚI

Într-o economie și o societate digitală interconectată, incidentele cibernetice nu se opresc la frontieră. Toți actorii, de la autoritățile competente din domeniul NIS, organismele CERT și organismele de aplicare a legii și până la industrie, trebuie să își asume responsabilitatea atât la nivel național, cât și la nivelul UE și să colaboreze în vederea întăririi securității cibernetice. Ținând cont de faptul că pot fi implicate diferite cadre juridice și jurisdicții, una dintre provocările majore ale UE este clarificarea rolurilor și a responsabilităților numeroșilor actori implicați.

Având în vedere complexitatea problemei și gama largă a actorilor implicați, supravegherea centralizată la nivel european nu este soluția potrivită. Administrațiile naționale sunt cele mai în măsură să organizeze activitățile de prevenire și reacție în caz de incidente și atacuri cibernetice. Tot ele sunt cele mai bine plasate pentru a crea contacte și rețele cu sectorul privat și publicul larg, grație canalelor administrative și cadrelor juridice de care dispun. În același timp, datorită caracterului transfrontalier potențial sau real al riscurilor, un răspuns eficace la nivel național ar necesita de multe ori o acțiune la nivelul UE. Pentru a aborda securitatea cibernetică în mod exhaustiv, activitățile ar trebui să acopere trei piloni principali — NIS, aplicarea legii și apărare – reglementați în același timp prin cadre juridice diferite:



3.1. Coordonarea dintre autoritățile competente în domeniul NIS/organismele CERT, organismele de aplicare a legii și organismele de apărare

La nivel național

Statele membre ar trebui să dispună, fie deja la ora actuală, fie în urma aplicării prezentei strategii, de structuri dedicate rezilienței cibernetice, criminalității cibernetice și apărării; aceste structuri ar trebui să atingă nivelul corespunzător în ceea ce privește capacitatea de a răspunde la incidentele cibernetice. Având în vedere însă faptul că o serie de entități pot avea responsabilități operaționale care acoperă domenii diferite ale securității cibernetice și ținând cont de importanța implicării sectorului privat, ar trebui optimizată coordonarea dintre ministere la nivel național. În cadrul strategiilor naționale privind securitatea cibernetică, statele membre ar trebui să precizeze rolurile și responsabilitățile diferitelor lor entități naționale.

Ar trebui încurajat schimbul de informații între entitățile naționale și cu sectorul privat, pentru a permite statelor membre și sectorului privat să păstreze o vedere de ansamblu asupra diferitelor amenințări și să dobândească o mai bună înțelegere a noilor tendințe și tehnici utilizate atât pentru a comite atacuri cibernetice, cât și pentru a le răspunde cu mai multă rapiditate. Prin definirea unor planuri naționale de cooperare în domeniul NIS, care trebuie activate în cazul producerii de incidente cibernetice, statele membre ar trebui să aibă posibilitatea de a atribui în mod clar rolurile și responsabilitățile și de a optimiza acțiunile de răspuns.

La nivelul UE

Ca și la nivel național, există la nivelul UE o serie de actori implicați în domeniul securității cibernetice. În particular, ENISA, Europol/EC3 și EDA sunt trei agenții active din punctele de vedere ale NIS, aplicării legii, respectiv apărării. Aceste agenții au consilii de administrație ce includ reprezentanți ai statelor membre și constituie platforme de coordonare la nivelul UE.

Coordonarea și colaborarea dintre ENISA, Europol/EC3 și EDA va fi încurajată într-o serie de domenii în care acestea sunt implicate în comun, în special în ceea ce privește analiza tendințelor, evaluarea riscurilor, formarea și schimbul de bune practici. Ele trebuie să colaboreze, păstrând-și în același timp specificitățile. Aceste agenții, împreună cu CERT-EU, Comisia și statele membre ar trebui să sprijine dezvoltarea unei comunități de încredere formate din experți pe probleme tehnice și de politică în domeniu.

Canalele neoficiale de coordonare și colaborare vor fi completate de legături mai structurate. Personalul militar al UE și echipa proiectului de apărare cibernetică a EDA pot fi utilizați ca vector de coordonare a apărării. Comitetul director al programului Europol/EC3 va reuni, printre alții, EUROJUST, CEPOL, statele membre[31], ENISA și Comisia și le va oferi posibilitatea de a-și împărtăși cunoștințele respective și de a se asigura că acțiunile EC3 sunt desfășurate în parteneriat, recunoscând contribuția la nivel de expertiză a tuturor părților interesate și respectând mandatele acestora. Noul mandat al ENISA ar trebui să-i permită acesteia strângerea legăturilor cu Europol și cu părțile interesate din industria de profil. Cel mai important, propunerea legislativă a Comisiei privind NIS ar stabili un cadru de cooperare prin intermediul unei rețele de autorități naționale competente în domeniul NIS și ar viza schimbul de informații dintre autoritățile de aplicare a legii și cele din domeniul NIS.

La nivel internațional

Comisia și Înaltul Reprezentant asigură, împreună cu statele membre, o acțiune internațională coordonată în domeniul securității cibernetice. În acest sens, Comisia și Înaltul Reprezentant vor susține valorile fundamentale ale UE și vor promova o utilizare pașnică, deschisă și transparentă a tehnologiilor cibernetice. Comisiei, Înaltul Reprezentant și statele membre angajează un dialog politic cu parteneri internaționali și cu organizații internaționale, cum ar fi Consiliul Europei, OCDE, OSCE, NATO și ONU.

3.2. Sprijinul UE în caz de incident sau atac cibernetic grav

Incidentele sau atacurile cibernetice grave sunt susceptibile de a avea un impact asupra administrațiilor naționale, întreprinderilor și cetățenilor UE. Strategia de față și în special propunerea de directivă privind NIS ar trebui să aibă ca rezultat ameliorarea prevenirii,

[31] Prin intermediul reprezentanților acestora în cadrul Grupului operativ al UE pentru combaterea criminalității cibernetice, care este alcătuit din șefii unităților de combatere a criminalității cibernetice ale UE din statele membre.

detectării și reacției la incidentele cibernetice, iar statele membre și Comisia vor trebui să se informeze reciproc cu mai multă atenție în legătură cu incidentele sau atacurile cibernetice grave Cu toate acestea, mecanismele de reacție vor fi diferite, în funcție de natura, amploarea și de implicațiile transfrontaliere ale incidentului.

Dacă incidentul are un impact grav asupra continuității activităților, directiva privind NIS propune declanșarea unor planuri de cooperare în materie de NIS la nivel național sau la nivelul Uniunii, în funcție de caracterul transfrontalier al acestui incident. În acest context, rețeaua autorităților competente în domeniul NIS va fi utilizată pentru schimbul de informații și pentru sprijin. Acest lucru ar urma să permită conservarea și/sau refacerea rețelelor și serviciilor afectate.

Dacă incidentul pare să aibă legătură cu o infracțiune, vor trebui informate Europol/EC3 pentru ca acestea, împreună cu autoritățile de aplicare a legii din țările afectate – să poată lansa o anchetă, să poată conserva probele, identifica autorii și, în cele din urmă, să poată garanta faptul că aceștia sunt urmăriți în justiție.

Dacă incidentul pare să se înscrie în categoria spionajului cibernetic ori a atacurilor comanditate de stat sau dacă el are repercusiuni asupra securității naționale, autoritățile naționale de securitate și apărare vor alerta omologii lor din alte țări, astfel încât aceștia să știe că sunt atacați și să se poată apăra. Vor fi apoi activate mecanismele de alertă rapidă, însoțite dacă este cazul de alte proceduri, cum ar fi cele de gestionare a crizelor. Un 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 (articolul 222 din Tratatul privind funcționarea Uniunii Europene).

Dacă incidentul pare să fi compromis date cu caracter personal, vor trebui implicate autoritățile naționale de protecție a datelor sau autoritatea națională de reglementare în conformitate cu Directiva 2002/58/CE.

În fine, gestionarea incidentelor și a atacurilor cibernetice, care poate include soluții tehnice de reducere a efectelor, anchete penale sau activarea mecanismelor de reacție și de gestionare a crizelor, va avea de câștigat datorită rețelelor de contact și a sprijinului acordat de partenerii internaționali.

4. CONCLUZIE ȘI FOLLOW-UP

Prezenta propunere de strategie de securitate cibernetică a Uniunii Europene, prezentată de Comisie și de Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate prezintă viziunea UE și acțiunile necesare, fondate pe protejarea și promovarea cu tărie a drepturilor cetățenilor, pentru a face astfel încât mediul online al UE să devină cel mai sigur din lume.[32]

[32] Finanțarea strategiei va fi asigurată în limita sumelor prevăzute pentru fiecare din domeniile de politică vizate (Facilitatea „Conectarea Europei ”, Orizont 2020, Fondul pentru securitate internă, PESC și cooperare externă, în special instrumentul de stabilitate), astfel cum este prevăzut în propunerea Comisiei privind cadrul financiar multianual 2014-2020 (sub rezerva aprobării de către autoritatea bugetară și a sumelor definitive ale CFM adoptat pentru perioada 2014-2020). În ceea ce privește necesitatea de a asigura compatibilitatea globală cu numărul de posturi disponibile pentru agențiile descentralizate și cu subplafonul fiecărei rubrici de cheltuieli a agențiilor descentralizate din următorul cadru financiar multianual, agențiile (CEPOL, EDA ENISA, EUROJUST și EUROPOL/EC3) cărora li se solicită, prin prezenta comunicare, să-și asume noi sarcini vor fi încurajate să facă acest lucru, în

Această viziune poate fi realizată doar cu ajutorul unui parteneriat real între numeroși actori, cu ajutorul căruia să fie asumate responsabilități și să se facă față provocărilor viitoare.

Comisia și Înaltul Reprezentant invită, prin urmare, Consiliul și Parlamentul European să aprobe strategia și să contribuie la realizarea acțiunilor prezentate. Este de asemenea nevoie de un sprijin și un angajament puternic din partea sectorului privat și a societății civile, care sunt actori-cheie în eforturile de sporire a nivelului nostru de securitate și de protejare a drepturilor cetățenilor.

Acum este momentul să acționăm. Comisia și Înaltul reprezentant sunt hotărâți să lucreze împreună cu toți actorii implicați, pentru a asigura Europei securitatea necesară. Pentru a garanta faptul că strategia este pusă în aplicare cu promptitudine și evaluată astfel încât să țină seama de posibilele evoluții, în termen de 12 luni ei vor reuni toate părțile interesate în cadrul unei conferințe la nivel înalt, unde se vor evalua progresele înregistrate.

măsura în care capacitatea agenției de a absorbi resurse în creștere a fost stabilită și toate posibilitățile de redistribuire au fost identificate.