COMISIA EUROPEANĂ

Bruxelles, 31.3.2011
COM(2011) 163 final

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

privind protecția infrastructurilor critice de informație

„Realizări și etape următoare: către un context global de securitate cibernetică

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

privind protecţia infrastructurilor critice de informaţie

„Realizări şi etape următoare: către un context global de securitate cibernetică”

1. INTRODUCERE

La 30 martie 2009, Comisia a adoptat o comunicare privind protecţia infrastructurilor critice de informaţie – „Protejarea Europei de atacuri cibernetice şi perturbaţii de amploare: ameliorarea gradului de pregătire, a securităţii şi a rezilienţei”[1] – prin care stabilea un plan („planul de acţiune privind protecţia infrastructurilor critice de informaţie”) în vederea consolidării securităţii şi rezilienţei infrastructurilor vitale ale tehnologiei informaţiei şi comunicaţiilor (TIC). Obiectivul era acela de a stimula şi sprijini dezvoltarea unui nivel ridicat al capacităţii de reacţie, de securitate şi de reziliență, atât la nivel naţional, cât şi la nivel european. Această abordare a fost aprobată în linii mari de către Consiliu în 2009[2].

Planul de acţiune privind protecţia infrastructurilor critice de informaţie este construit pe cinci piloni: pregătirea şi prevenirea, depistarea şi reacţia, reducerea riscurilor şi redresarea după incidente, cooperarea internaţională şi criteriile pentru infrastructurile critice europene din sectorul TIC. Acesta stabileşte măsurile care trebuie luate în legătură cu fiecare pilon de Comisie, statele membre şi/sau industrie, cu sprijinul Agenţiei Europene pentru Securitatea Reţelelor Informatice şi a Datelor (ENISA).

Agenda digitală pentru Europa[3], adoptată în mai 2010, şi concluziile aferente ale Consiliului[4] au subliniat viziunea comună conform căreia încrederea şi securitatea sunt condiţii prealabile fundamentale pentru utilizarea la scară largă a tehnologiei informaţiei şi comunicaţiilor şi pentru realizarea în acest fel a obiectivelor vizate de dimensiunea „creştere inteligentă” a Strategiei Europa 2020[5]. Agenda digitală pentru Europa subliniază necesitatea ca toate părţile interesate să-şi unească forţele într-un efort global pentru a garanta securitatea şi reziliența infrastructurilor TIC, prin acordarea unei importanţe speciale prevenirii, gradului de pregătire şi sensibilizării, precum şi pentru a dezvolta mecanisme eficiente şi coordonate ca să poată reacţiona la formele din ce în ce mai sofisticate de atacuri şi infracţiuni cibernetice. Această abordare garantează că atât dimensiunea preventivă, cât şi cea de reacţie, sunt provocări de care se ţine seama în mod corespunzător.

Următoarele măsuri, anunţate în Agenda digitală, au fost luate în ultimele luni: Comisia a adoptat în septembrie 2010 o propunere de directivă privind atacurile împotriva sistemelor de

---

1 COM(2009) 149.

2 Rezoluţia Consiliului din 18 decembrie 2009 privind o abordare europeană a securităţii reţelelor şi a informaţiilor bazată pe colaborare (2009/C 321/01).

3 COM(2010) 245.

4 Concluziile Consiliului din 31 mai 2010 privind Agenda digitală pentru Europa (10130/10).

5 COM(2010) 2020 şi Concluziile Consiliului European din 25 şi 26 martie 2010 (EUCO 7/10).

informații[6]. Aceasta vizează consolidarea luptei împotriva atacurilor cibernetice prin apropierea sistemelor de drept penal ale statelor membre și prin îmbunătățirea cooperării între autoritățile judiciare și alte autorități competente. De asemenea, propunerea introduce unele dispoziții privind modalitatea de combatere a noilor forme de atacuri cibernetice, în speță botneturile. Comisia a înaintat în același timp și o propunere[7] pentru un nou mandat de consolidare și modernizare a Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) în vederea creșterii gradului de încredere și a securității rețelelor. Consolidarea și modernizarea ENISA va permite Uniunii Europene, statelor membre și părților interesate din sectorul privat să își dezvolte capacitățile și pregătirea în vederea prevenirii, detectării și abordării provocărilor care țin de securitatea informatică.

Și nu în ultimul rând, Agenda digitală pentru Europa, Programul de la Stockholm/planul de acțiune al acestuia[8] și Strategia de securitate internă a UE în acțiune[9] subliniază angajamentul Comisiei de a construi un mediu digital în care toți europenii să-și poată exprima întregul potențial economic și social.

Prezenta comunicare face bilanțul rezultatelor obținute de la adoptarea planului de acțiune privind protecția infrastructurilor critice de informație în 2009. Ea descrie măsurile viitoare preconizate pentru fiecare acțiune, atât la nivel european, cât și internațional și se concentrează, totodată, asupra dimensiunii globale a provocărilor și a importanței intensificării cooperării dintre administrațiile statelor membre și sectorul privat la nivel național, european și internațional, pentru a se trata interdependențele la nivel global.

2. UN SCENARIU ÎN CONTINUĂ EVOLUȚIE

Evaluarea impactului care însoțește planul de acțiune privind protecția infrastructurilor critice de informație[10], precum și o serie de analize și rapoarte realizate de părțile interesate din sectorul public și privat subliniază nu doar dependența socială, politică și economică de TIC a Europei, ci și creșterea constantă a numărului, amplorii, gradului de sofisticare și a impactului amenințărilor, fie că e vorba de amenințări naturale sau generate de oameni.

Au apărut amenințări noi și mai sofisticate din punct de vedere tehnologic. Dimensiunea geopolitică globală a acestora devine din ce în ce mai clară. Asistăm în prezent la o tendință de utilizare a tehnologiilor informației și comunicațiilor în scopul supremației politice, economice și militare, inclusiv prin capacități ofensive. „Războiul cibernetic” și „terorismul cibernetic” sunt uneori menționate în acest context.

În plus, după cum o arată și recentele evenimente sud-mediteraneene, unele regimuri sunt pregătite și capabile să interzică sau să submineze în mod arbitrar accesul propriilor lor cetățeni la mijloacele informatice de comunicare – în special internetul și comunicațiile mobile – în scopuri politice. Astfel de intervenții interne unilaterale pot avea consecințe grave asupra altor părți ale lumii[11].

---

6 COM(2010) 517 final.
7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.
11 Comunicare comună privind Parteneriatul pentru democrație și prosperitate împărtășită cu țările sud-mediteraneene, COM(2011) 200, 8.3.2011.

Pentru a înțelege și mai bine aceste diferite amenințări, poate fi util să le împărțim în următoarele categorii:

– pentru **exploatare**, cum ar fi „amenințările avansate persistente”[12], în scopul spionajului economic și politic (de exemplu, GhostNet[13]), furtul de identitate, recentele atacuri împotriva sistemului de comercializare a cotelor de emisii[14] sau împotriva sistemelor informatice guvernamentale[15];

– pentru **sabotaj**, cum ar fi atacurile de tip DDoS (*Distributed Denial of Service* – blocarea distribuită a serviciului) sau spamurile generate prin botneturi (de exemplu, rețeaua Conficker de 7 milioane de calculatoare și rețeaua Mariposa din Spania de 12,7 milioane de calculatoare[16]), Stuxnet[17] și întreruperea mijloacelor de comunicare;

– pentru **distrugere**. Acesta este un scenariu care încă nu s-a materializat, însă, dată fiind utilizarea crescândă a TIC în infrastructurile critice (de exemplu, rețelele inteligente și rețelele de distribuție a apei), el nu este exclus pentru anii care vin[18].

3. UNIUNEA EUROPEANĂ ȘI CONTEXTUL GLOBAL

Provocările viitoare nu sunt specifice Uniunii Europene (UE) și nici nu pot fi rezolvate doar de UE. Gradul din ce în ce mai ridicat de utilizare a TIC și a internetului permite o comunicare, o coordonare și o cooperare mai eficientă, rentabilă și economică între părțile interesate și are drept rezultat un ecosistem dinamic de inovare în toate domeniile vieții. În prezent însă, amenințările pot apărea în orice parte a lumii și, din cauza interconectării globale, pot afecta orice parte a lumii.

O abordare doar la nivel european nu este suficientă pentru soluționarea problemelor viitoare. Deși obiectivul realizării unei abordări bazate pe coerență și cooperare în cadrul UE rămâne la fel de important ca întotdeauna, el trebuie să se înscrie într-o strategie de coordonare globală care să includă partenerii cheie, fie că este vorba de națiuni sau de organizații internaționale.

Trebuie să avansăm în direcția conștientizării la nivel mondial a riscurilor pe care le presupune utilizarea masivă de către toate segmentele societății a tehnologiilor informațiilor și comunicațiilor. Mai mult, trebuie să concepem strategii pentru a gestiona aceste riscuri în mod adecvat și eficient, fie că este vorba de prevenirea, combaterea, reducerea sau abordarea lor. Agenda digitală pentru Europa lansează o invitație pentru „*organizarea cooperării actorilor*

---

12 Și anume, atacurile neîntrerupte și coordonate împotriva agențiilor guvernamentale și sectorului public. Sunt pe cale să devină o problemă și pentru sectorul privat (a se vedea „Raportul RSA din 2011 privind tendințele infracționalității cibernetice”).

13 A se vedea rapoartele proiectului *Information Warfare Monitor*: „*Tracking GhostNet: investigating a Cyber Espionage Network*” (2009) și „*Shadows in the Cloud: Investigating Cyber Espionage 2.0*” (2010).

14 A se vedea întrebările și răspunsurile de la adresa: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Cum ar fi recentele atacuri împotriva guvernului francez.

16 A se vedea proiectul OCDE/IFP privind „Șocurile globale viitoare” și „Reducerea riscurilor sistemice la adresa securității cibernetice”, 14 ianuarie 2011, la adresa http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 A se vedea http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 A se vedea *World Economic Forum, Global Risks 2011*.

relevanți [...] la nivel global pentru ca aceștia să fie în măsură să combată și să reducă riscurile la adresa securității" și stabilește obiectivul de a „*coopera cu părțile interesate la nivel mondial pentru consolidarea* ***gestionării globale a riscurilor*** *în sfera digitală și cea fizică și pentru adoptarea de măsuri specifice coordonate la nivel internațional împotriva infracțiunilor informatice și a atacurilor la adresa securității*".

4. PUNEREA ÎN APLICARE A PLANULUI DE ACȚIUNE PRIVIND PROTECȚIA INFRASTRUCTURILOR CRITICE DE INFORMAȚIE: IDEI GENERALE

Raportul integral referitor la realizările și etapele următoare ale planului de acțiune privind protecția infrastructurilor critice de informație este disponibil în anexă. În continuare sunt enumerate câteva idei generale privind starea de fapt.

4.1. Pregătirea și prevenirea

- **Forumul european al statelor membre** (FESM) a înregistrat progrese semnificative în stimularea dialogului și a schimburilor dintre autoritățile de resort cu privire la bunele practici în materie de politici legate de securitatea și reziliența infrastructurilor TIC. Forumul european al statelor membre este recunoscut de statele membre drept o platformă importantă pentru discuții și schimburi de bune practici în materie de politici[19]. Activitățile sale viitoare vor beneficia în continuare de sprijinul ENISA și se vor concentra asupra cooperării dintre echipele naționale/guvernamentale de intervenție în caz urgență informatică (*Computer Emergency Response Teams* – CERT), prin identificarea stimulentelor economice și de reglementare pentru securitate și reziliență (respectându-se în același timp și normele în vigoare în materie de concurență și ajutoare de stat), prin evaluarea stării de „sănătate a securității cibernetice" în Europa, prin organizarea de exerciții paneuropene, precum și prin discutarea priorităților de abordat într-un cadru internațional cu privire la securitate și reziliență.

- **Parteneriatul european public-privat pentru reziliență** (EP3R) a fost lansat drept cadru european de guvernanță pentru reziliența infrastructurilor TIC. Acesta vizează dezvoltarea cooperării dintre sectorul public și cel privat în chestiuni politice și strategice la nivelul UE legate de securitate și reziliență. ENISA a jucat rolul de mediator pentru activitățile EP3R și, în urma propunerii Comisiei din 2010 privind modernizarea ENISA, aceasta va oferi un cadru viabil pe termen lung pentru EP3R. EP3R va reprezenta totodată o platformă de anvergură internațională pentru chestiunile de politici publice și pentru problemele economice și comerciale care sunt relevante în ceea ce privește securitatea și reziliența, pentru a consolida gestionarea globală a riscurilor privind infrastructurile TIC.

- Au fost stabilite atât **baza minimă de capacități și servicii**[20], cât și **recomandările de politici** aferente acesteia[21], necesare pentru ca CERT naționale/guvernamentale să își desfășoare activitatea în mod eficient și să acționeze ca o componentă cheie a capacității

---

19 Răspunsul guvernului britanic la cel de-al cincilea raport al Comisiei pentru Uniunea Europeană a Camerei Lorzilor referitor la planul de acțiune privind protecția infrastructurilor critice de informație declară că Forumul european al statelor membre „*reprezintă un succes și răspunde unei nevoi reale, oferind factorilor de decizie ocazia de a face schimb de experiență*".

20 A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

naționale în ceea ce privește pregătirea, schimbul de informații, coordonarea și reacția. Aceste rezultate vor constitui baza pe care se va institui, cu sprijinul ENISA, o rețea de CERT naționale/guvernamentale care să funcționeze eficient în toate statele membre cel târziu până în 2012. Această rețea va reprezenta coloana vertebrală a Sistemului european de alertă și schimb de informații (EISAS) pentru cetățeni și IMM-uri, care urmează a fi construit cu resurse și capacități naționale până în 2013.

4.2. Depistarea și reacția

- ENISA a stabilit o foaie de parcurs la nivel înalt pentru instituirea unui Sistem european de alertă și schimb de informații (**EISAS**) până în 2013[22], pornind de la implementarea *serviciilor de bază* la nivelul CERT naționale/guvernamentale și a *serviciilor de interoperabilitate* pentru sistemele naționale de alertă și schimb de informații care urmează a fi integrate în EISAS. Protecția corespunzătoare a datelor cu caracter personal va fi unul dintre elementele cheie ale acestei activități.

4.3. Reducerea riscurilor și redresarea după incidente

- Până în prezent, doar 12 state membre au organizat exerciții legate de reacția la incidentele de mare anvergură care afectează securitatea rețelelor și de redresarea după dezastre[23]. Pentru a sprijini activitățile statelor membre, care trebuie intensificate, ENISA a publicat **un ghid de bune practici pentru exercițiile naționale**[24], precum și **o serie de recomandări de politici** cu privire la elaborarea de strategii naționale[25].

- Primul **exercițiu paneuropean legat de incidentele de mare anvergură care afectează securitatea rețelelor** (denumit *Cyber Europe 2010*) a avut loc la 4 noiembrie 2010 cu participarea tuturor statelor membre, dintre care 19 au luat parte la exercițiu în mod activ, acestor țări alăturându-li-se Elveția, Norvegia și Islanda. Exercițiile informatice paneuropene viitoare ar beneficia fără îndoială de pe urma unui cadru comun care să aibă drept fundament planurile naționale de intervenție, cu care s-ar interconecta, oferind în acest fel mecanisme și proceduri de referință pentru comunicarea și cooperarea dintre statele membre.

4.4. Cooperarea internațională

- **Principiile și orientările europene pentru reziliența și stabilitatea internetului**[26] au fost discutate și dezvoltate în contextul FESM. Comisia va discuta aceste principii și le va prezenta părților interesate relevante, în special sectorului privat (prin EP3R), atât pe plan bilateral cu partenerii cheie la nivel internațional, în speță SUA, cât și pe plan multilateral. Ea va face acest lucru, în sfera sa de competență, în foruri precum G8, OCDE, NATO (în special pe baza noului său concept strategic adoptat în noiembrie 2010 și a activităților centrului de excelență pentru cooperare în domeniul apărării cibernetice, *Cooperative Cyber-defense Center of Excellence*), ITU (în contextul consolidării capacităților în

---

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Sursa: ENISA.

24 A se vedea http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 A se vedea http://ec.europa.eu/information_society/policy/nis/index_en.htm

domeniul securității cibernetice), OSCE (prin intermediul Forumului pentru cooperare în materie de securitate), ASEAN, Meridian[27] etc. Obiectivul este de a integra aceste principii și orientări într-un cadru comun care să promoveze angajamentul colectiv internațional pentru reziliența și stabilitatea pe termen lung a internetului.

4.5. Criterii pentru infrastructurile critice europene din sectorul TIC

- Discuțiile tehnice din cadrul FESM au dus la un **prim proiect al criteriilor specifice sectorului TIC** pentru identificarea infrastructurilor critice europene, cu referire în special **la comunicațiile fixe și mobile și la internet**. Aceste discuții tehnice vor continua și vor beneficia de pe urma consultărilor cu sectorul privat, cu privire la proiectul de criterii, atât la nivel național, cât și european (prin EP3R). De asemenea, Comisia va analiza împreună cu statele membre elementele specifice ale sectorului TIC care trebuie avute în vedere pentru revizuirea Directivei privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora[28] în 2012.

5. ETAPE VIITOARE

Implementarea planului de acțiune privind protecția infrastructurilor critice de informație a înregistrat rezultate pozitive, în special în ceea ce privește recunoașterea necesității unei abordări a securității rețelelor și informațiilor care să se bazeze pe cooperare și să implice toate părțile interesate. Ea este totodată în concordanță cu etapele principale și cu termenele stabilite în 2009. Cu toate acestea, nu trebuie să ne mulțumim doar cu ce s-a întreprins până acum, dat fiind că mai sunt multe rezultate de obținut atât la nivel național, cât și european, pentru ca toate aceste eforturi să aducă roade.

De asemenea, este foarte important ca eforturile de întreprins să fie incluse într-o strategie de coordonare globală astfel încât acestea să poată fi extinse la nivel internațional, cu toate părțile interesate, pentru a fi implicate și alte regiuni, țări sau organizații care se confruntă cu probleme similare și pentru ca astfel să se dezvolte parteneriate prin care să se pună în comun perspectivele și activitățile și să se evite duplicarea eforturilor.

Este necesar să promovăm o cultură globală a gestionării riscurilor. Trebuie pus accentul pe promovarea acțiunilor coordonate pentru a preveni, a detecta, a reduce orice nereguli și a reacționa la acestea, fie că este vorba de probleme naturale sau generate de om, precum și pentru a se pedepsi infracțiunile cibernetice. Acest lucru presupune realizarea de acțiuni specifice pentru a combate riscurile la adresa securității și a infracțiunilor informatice.

În acest scop, **Comisia intenționează**:

- **să promoveze principiile pentru reziliența și stabilitatea internetului** – ar trebui dezvoltate principii internaționale pentru reziliența și stabilitatea internetului împreună cu alte țări, cu alte organizații internaționale și, dacă este cazul, cu organizațiile mondiale din sectorul privat, cu ajutorul forurilor și proceselor existente, cum ar fi cele legate de guvernanța internetului. Aceste principii ar trebui să reprezinte un instrument pe care toate

---

[27] Procesul Meridian își propune să ofere guvernelor din întreaga lume mijloacele prin care acestea să poată discuta modalitățile de cooperare la nivel de politici cu privire la protecția infrastructurilor critice de informație. A se vedea http://meridianprocess.org/

[28] Directiva 2008/114/CE a Consiliului.

părțile interesate să-l folosească pentru definirea activităților legate de stabilitatea și reziliența internetului. În acest scop, principiile și orientările europene pot servi drept bază.

- **să instituie parteneriate strategice internaționale** – parteneriatele strategice ar trebui să pornească de la eforturile în curs în domeniile critice, cum ar fi gestionarea incidentelor cibernetice, inclusiv exercițiile și cooperarea dintre echipele de intervenție în caz urgență informatică. Angajamentul sectorului privat, care se realizează la scară globală, prezintă o importanță majoră. Grupul de lucru UE-SUA privind securitatea și infracționalitatea cibernetică, înființat cu ocazia summitului UE-SUA din noiembrie 2010, este o etapă importantă în această direcție. Grupul de lucru se va concentra asupra gestionării incidentelor cibernetice, parteneriatelor public-privat, sensibilizării populației și infracționalității cibernetice. De asemenea, el ar putea avea în vedere opțiuni pentru a include și alte regiuni sau țări, care se confruntă cu probleme similare, în vederea punerii în comun a practicilor și a activităților conexe și pentru a se evita duplicarea eforturilor, dacă este cazul. În forurile internaționale, în special în cadrul G8, ar trebui să se urmărească un grad mai mare de includere și coordonare. La nivel european, un factor cheie de succes va fi buna coordonare dintre toate instituțiile UE, agențiile de resort (în special ENISA și Europol) și statele membre.

- **să crească gradul de încredere în mediul informatic dematerializat („cloud")** – este esențială consolidarea discuțiilor privind cele mai bune strategii de guvernanță pentru tehnologiile emergente cu un impact global, cum ar fi cloud computing-ul. Aceste discuții ar trebui cu siguranță să includă, printre altele, cadrul adecvat de guvernanță pentru protecția datelor cu caracter personal. Pentru a se exploata pe deplin această tehnologie, încrederea este un factor esențial[29].

Dat fiind că securitatea reprezintă o responsabilitate comună tuturor, toate statele membre trebuie să se asigure că măsurile și eforturile lor la nivel național vor contribui în mod colectiv la o abordare europeană coordonată, în vederea prevenirii, reducerii și abordării oricăror tipuri de nereguli și atacuri cibernetice. În acest sens, **statele membre trebuie să se angajeze**:

- **să crească gradul de pregătire a UE, prin instituirea, până în 2012, a unei rețele de CERT naționale/guvernamentale care să funcționeze corespunzător.** În același timp, instituțiile UE vor înființa CERT la nivelul lor până în 2012. Toate aceste eforturi ar trebui să se sprijine pe baza minimă de capacități și servicii corespunzătoare și pe recomandările de politici aferente redactate de ENISA, care va continua să susțină aceste inițiative. Totodată, această activitate va prezenta publicului larg evoluția Sistemului european de alertă și schimb de informații (EISAS) până în 2013.

- **să elaboreze, până în 2012, un plan de intervenție în caz de incidente cibernetice și să efectueze exerciții cibernetice periodice paneuropene.** Exercițiile cibernetice reprezintă o componentă importantă a unei strategii coerente privind elaborarea de planuri de intervenție în caz de incidente cibernetice și de redresare în urma acestora, atât la nivel național, cât și european. Viitoarele exerciții cibernetice paneuropene ar trebui să se bazeze pe un plan european de intervenție în caz de incidente cibernetice care să aibă drept bază

[29] A se vedea, de exemplu, rapoartele ENISA intitulate „Cadrul de asigurare a informațiilor în cloud computing" (2009), la adresa http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport și „Securitatea și reziliența în mediul cloud guvernamental" (2011), la adresa http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

planurile naționale de intervenție, cu care să se interconecteze. Acest plan ar trebui să ofere mecanismele și procedurile de bază pentru comunicarea dintre state membre și, nu mai puțin important, să sprijine amploarea și organizarea viitoarelor exerciții paneuropene. ENISA va colabora cu statele membre pentru a elabora, până în 2012, acest plan european de intervenție în caz de incidente cibernetice. În aceeași perioadă, toate statele membre vor trebui să elaboreze periodic planuri naționale de intervenție, precum și exerciții de reacție la incidente și redresare în urma acestora.

- **să întreprindă eforturi coordonate la nivel european în forurile internaționale și să instituie un dialog cu privire la ameliorarea securității și rezilienței internetului.** Statele membre trebuie să conlucreze și să colaboreze cu Comisia pentru a promova dezvoltarea unei abordări bazate pe principii sau norme în ceea ce privește chestiunea stabilității și rezilienței globale a internetului. Scopul trebuie să fie acela de a promova prevenirea și pregătirea la toate nivelurile și de către toate părțile interesate, echilibrând astfel tendința actuală a discuțiilor care se concentrează asupra aspectelor militare sau de securitate națională.

6. CONCLUZIE

Experiența ne arată că abordările la nivel exclusiv național sau regional în vederea soluționării problemelor legate de securitate și reziliență nu sunt suficiente. Cooperarea europeană s-a dezvoltat semnificativ începând din 2009 și a înregistrat rezultate încurajatoare, cum este de pildă exercițiul *Cyber Europe 2010*. Însă Europa trebuie să-și continue eforturile pentru a pune în practică o abordare coerentă și bazată pe cooperare în întreaga UE. În urma modernizării, Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor ar urma să fie în măsură să intensifice sprijinul acordat statelor membre, instituțiilor UE și sectorului privat pentru eforturile pe termen lung ale acestora.

Pentru a aduce roade, eforturile europene trebuie să se înscrie într-o abordare coordonată la nivel global. În acest scop, Comisia va promova dialogul cu privire la securitatea cibernetică în toate forurile internaționale corespunzătoare.

O conferință ministerială pe tema protecției infrastructurilor critice de informație, organizată de președinția ungară a UE, va avea loc în data de 14-15 aprilie 2011. Această conferință reprezintă o ocazie importantă de a consolida angajamentul pentru cooperarea și coordonarea mai strânsă între statele membre, atât la nivel european, cât și la nivel internațional.

ANEXĂ

Planul de acțiune privind protecția infrastructurilor critice de informație: prezentarea detaliată a realizărilor și a etapelor următoare

Rezultatele activităților realizate în contextul planului de acțiune privind protecția infrastructurilor critice de informație sunt în concordanță cu etapele principale și cu termenele stabilite de Comisie în 2009. În continuare sunt descrise „realizările” și „etapele următoare” în ceea ce privește toți pilonii. Această prezentare ține seama de faptul că anumite activități au fost analizate mai în detaliu în Agenda digitală pentru Europa și în Strategia de securitate internă a UE în acțiune.

1. Pregătirea și prevenirea

Nivelul de bază comun de capacități și servicii pentru cooperarea paneuropeană

Realizări

– În 2009, ENISA și comunitatea echipelor de intervenție în caz urgență informatică (CERT) din Europa au dezbătut și convenit asupra unui set minim de capacități și servicii de bază de care echipele naționale/guvernamentale de intervenție în caz urgență informatică trebuie să dispună pentru a putea acționa eficient în sprijinul cooperării paneuropene. S-a ajuns la un consens referitor la o listă de elemente obligatorii în ceea ce privește operarea, capacitățile tehnice, mandatul și cooperarea[30].

– În 2010, ENISA a colaborat cu comunitatea CERT din Europa pentru a transforma cerințele operaționale de mai sus într-un set de recomandări de politici[31] pentru ca CERT naționale/guvernamentale să acționeze ca o componentă cheie a capacității naționale de pregătire, schimb de informații, coordonare și reacție.

– Până în prezent, 20 de state membre[32] au înființat CERT naționale/guvernamentale și aproape toate celelalte au planificat să înființeze astfel de echipe. Așa cum s-a anunțat în Agenda digitală pentru Europa și după cum s-a precizat și în Strategia de securitate internă a UE în acțiune, Comisia a propus măsuri pentru ca, până în 2012, să se înființeze echipe de intervenție în caz urgență informatică pentru instituțiile UE.

Etapele următoare

– ENISA va continua să sprijine statele membre care nu au înființat încă CERT naționale/guvernamentale care să respecte cerințele de bază convenite, menționate anterior, pentru a garanta realizarea obiectivului unor CERT naționale/guvernamentale care să funcționeze eficient în toate statele membre până la sfârșitul anului 2011. Această etapă va pregăti instituirea unei rețele eficiente de CERT la nivel național **până în 2012**, după cum se prevede în Agenda digitală pentru Europa.

---

30 A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Sursa: ENISA.

– ENISA, în colaborare cu CERT naționale/guvernamentale, va analiza necesitatea și modalitățile de extindere a „capacităților de bază” pentru a adapta capacitatea CERT de a sprijini statele membre în garantarea rezilienței și stabilității infrastructurilor TIC vitale și pentru a deveni coloana vertebrală a Sistemului european de alertă și schimb de informații (EISAS) pentru cetățeni și IMM-uri, care urmează a fi construit cu resurse și capacități naționale **până în 2013**, după cum s-a anunțat în Strategia de securitate internă a UE în acțiune.

Parteneriatul public-privat european pentru reziliență (EP3R)

Realizări

– EP3R a fost lansat în 2009 drept cadrul de guvernanță la nivel european pentru reziliența infrastructurilor TIC, stimulând cooperarea dintre sectorul public și cel privat în ceea ce privește obiectivele de securitate și reziliență, cerințele de bază, bunele practici și măsuri de politici. Totodată, așa cum se precizează în Strategia de securitate internă a UE în acțiune, EP3R „*va coopera cu parteneri internaționali pentru consolidarea gestionării mondiale a riscului în materie de rețele informatice*”. ENISA facilitează activitatea EP3R.

– Părțile interesate din sectorul public și din cel privat au fost consultate pentru a se stabili obiectivele, principiile și structura EP3R și pentru a se determina care sunt stimulentele care ar putea încuraja părțile interesate relevante să se implice în mod activ[33]. În propunerea privind modernizarea ENISA au fost identificate domenii prioritare pentru EP3R[34].

– În paralel cu elaborarea structurii EP3R, la sfârșitul anului 2010 au fost lansate trei grupuri de lucru cu privire la (a) avantajele cheie, resursele și funcțiile ofertei continue și sigure de comunicații electronice în toate statele; (b) cerințe de bază pentru securitatea și reziliența comunicațiilor electronice; (c) necesitățile de coordonare și cooperare și mecanismele de pregătire și reacție în ceea ce privește neregulile la scară largă care afectează comunicațiile electronice.

– În 2010, propunerea Comisiei de modernizare a ENISA a oferit un cadru viabil pe termen lung pentru EP3R: aceasta propunea ca ENISA să „*sprijine cooperarea între părțile interesate din sectorul public și privat la nivelul Uniunii prin promovarea, printre altele, a schimbului de informații și a sensibilizării, și prin facilitarea eforturilor lor de a dezvolta și adopta standarde în materie de gestionare a riscului și de securitate a produselor, rețelelor și serviciilor electronice*”.

Etapele următoare

– În 2011, EP3R va continua să consolideze cooperarea dintre părțile interesate din sectorul public și cel privat în vederea îmbunătățirii securității și rezilienței prin măsuri și instrumente inovatoare și a definirii responsabilității părților interesate. Grupurile de lucru EP3R vor obține primele rezultate cu ajutorul medierii și sprijinului ENISA. Activitatea viitoare va aborda și riscurile la adresa securității cibernetice cu care se pot confrunta rețelele inteligente, pornind de la lucrările pregătitoare realizate de Comisie și de ENISA.

[33] A se vedea http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

[34] COM(2010) 521.

– EP3R va constitui o platformă pentru o abordare globală a politicilor publice și a chestiunilor economice și comerciale relevante pentru securitate și reziliență. Comisia intenționează să utilizeze EP3R pentru a veni în sprijinul activităților Grupului de lucru UE-USA privind securitatea și infracționalitatea cibernetică, pentru a oferi un mediu coerent pentru cooperare între sectorul public și privat, respectând în același timp normele în vigoare în materie de concurență și ajutoare de stat.

– Pe termen lung și în concordanță cu propunerea privind un nou Regulament referitor la ENISA, se preconizează că EP3R va deveni o activitate cheie în cadrul unei ENISA modernizate.

Forumul european al statelor membre (FESM)

Realizări

– FESM a fost înființat în 2009 pentru a promova discuțiile și schimburile privind bunele practici în materie de politici între autoritățile publice relevante, cu scopul de a se pune în comun obiective și priorități de politici privind securitatea și reziliența infrastructurilor TIC și a beneficiat de asemenea în mod direct de pe urma activității și a sprijinului oferit de ENISA. FESM, care se întrunește trimestrial, dispune, începând de la mijlocul anului 2010, de un portal web dedicat, administrat de ENISA.

– FESM a înregistrat progrese semnificative în ceea ce privește: (a) definirea criteriilor de identificare a infrastructurilor TIC europene în contextul Directivei privind identificarea și desemnarea infrastructurilor critice europene[35]; (b) identificarea priorităților, principiilor și orientărilor europene pentru reziliența și stabilitatea internetului; (c) schimbul de bune practici în materie de politici, în special în ceea ce privește exercițiile cibernetice.

– Forumul european al statelor membre este recunoscut de statele membre drept o platformă importantă pentru discuții și schimburi de bune practici în materie de politici[36].

Etapele următoare

– În 2011, FESM va finaliza discuțiile tehnice privind criteriile TIC pentru infrastructurile critice europene și va furniza orientările și prioritățile pe termen lung pentru exercițiile paneuropene la scară largă legate de securitatea rețelelor și a informațiilor.

– FESM se va implica în continuare în discuțiile privind prioritățile de anvergură internațională în materie de securitate și reziliență, în special în ceea ce privește activitățile Grupului de lucru UE-SUA privind securitatea și infracționalitatea cibernetică.

– Domeniile prioritare pentru acțiunile viitoare ale FESM, care vor beneficia de sprijinul direct al ENISA, includ[37]: elaborarea de metode pentru o colaborare eficace între CERT naționale/guvernamentale; utilizarea cerințelor minime privind achizițiile publice pentru a stimula securitatea cibernetică; identificarea stimulentelor economice și de reglementare în

35 Directiva 2008/114/CE a Consiliului.

36 Răspunsul guvernului britanic la cel de-al cincilea raport al Comisiei pentru Uniunea Europeană a Camerei Lorzilor referitor la planul de acțiune privind protecția infrastructurilor critice de informație declară că Forumul european al statelor membre „*reprezintă un succes și răspunde unei nevoi reale, oferind factorilor de decizie ocazia de a face schimb de experiență*".

37 COM(2010) 251.

favoarea securității și rezilienței (respectând în același timp și normele în vigoare în materie de concurență și ajutoare de stat); evaluarea stării de „sănătate a securității cibernetice” în Europa.

2. Depistare și reacție

Sistemul european de alertă și schimb de informații (EISAS)

Realizări

– Două proiecte prototip (FISHAS și NEISAS) au fost finanțate de Comisie și produc în prezent ultimele rezultate.

– Bazându-se pe raportul de fezabilitate din 2007[38] și pe analiza proiectelor relevante la nivel național și european, ENISA a conceput o foaie de parcurs la nivel înalt pentru dezvoltarea EISAS până în 2013[39].

Etapele următoare

– În 2011, ENISA va sprijini statele membre în procesul de implementare a foii de parcurs privind EISAS prin dezvoltarea „serviciilor de bază” de care statele membre au nevoie pentru înființarea sistemelor lor naționale de alertă și schimb de informații pe baza capacității CERT naționale/guvernamentale.

– În 2012, ENISA va dezvolta „serviciile de interoperabilitate”, făcând astfel posibilă integrarea funcțională în EISAS a tuturor sistemelor naționale de alertă și schimb de informații. ENISA va sprijini totodată statele membre în procesul de testare a acestor servicii prin integrarea progresivă a sistemelor naționale.

– În cursul perioadei 2011-2012, ENISA va stimula CERT naționale/guvernamentale să integreze în serviciile lor capacitatea sistemelor de alertă și schimb de informații.

3. Reducerea riscurilor și redresarea după incidente

Elaborarea planurilor de intervenție și exercițiile la nivel național

Realizări

– La sfârșitul anului 2010, 12 state membre elaboraseră un plan național de intervenție și/sau organizaseră exerciții legate de reacția la incidentele de mare anvergură care afectează securitatea rețelelor și de redresare după dezastre[40].

– Pe baza experiențelor naționale și internaționale, ENISA a elaborat un ghid de bune practici pentru exercițiile naționale[41]; a organizat diferite evenimente cu participarea statelor membre și a CERT din întreaga lume consacrate exercițiilor naționale; și, mai

38 A se vedea http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

40 A se vedea http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 A se vedea http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

recent, a publicat recomandări de politici pe tema elaborării de strategii naționale în care CERT/CSIRT (*Computer Security Incident Response Team* – echipe de intervenție în caz de incidente legate de securitatea informatică) naționale/guvernamentale au un rol cheie în gestionarea exercițiilor și testelor legate de planurile naționale de intervenție, cu implicarea părților interesate din sectorul privat și public[42].

Etapele următoare

– ENISA va continua să sprijine statele membre în efortul acestora de a elabora planuri naționale de intervenție și de a organiza periodic exerciții legate de reacția la incidentele de mare anvergură care afectează securitatea rețelelor și de redresarea după dezastre, în vederea ameliorării coordonării paneuropene.

Exerciții la nivel paneuropean privind incidentele de mare anvergură care afectează securitatea rețelelor

Realizări

– Primul exercițiu paneuropean legat de incidentele de mare anvergură care afectează securitatea rețelelor (*Cyber Europe 2010*) a avut loc la 4 noiembrie 2010 cu participarea tuturor statelor membre, dintre care 19 au luat parte la exercițiu în mod activ, acestor țări alăturându-li-se Elveția, Norvegia și Islanda. Exercițiul a fost organizat și evaluat[43] de ENISA, cu participarea activă a opt state membre, care au făcut parte din echipa de planificare, și cu sprijinul tehnologic al Centrului Comun de Cercetare (JRC).

Etapele următoare

– În 2011, statele membre vor demara discuțiile referitoare la obiectivul și amploarea următorului exercițiu cibernetic paneuropean planificat pentru 2012. Se va analiza opțiunea unei abordări pe etape, cu exerciții mai aprofundate, care să implice un grup mai restrâns de state membre și la care să participe eventual și actori internaționali. ENISA va continua să sprijine acest proces.

– Comisia sprijină financiar proiectul EuroCybex, care se referă la realizarea unui exercițiu de simulare în a doua jumătate a anului 2011.

– Exercițiile cibernetice reprezintă o componentă importantă a unei strategii coerente privind elaborarea de planuri de intervenție în caz de incidente cibernetice, atât la nivel național, cât și european. Prin urmare, viitoarele exerciții cibernetice paneuropene ar trebui să se bazeze pe un plan european de intervenție în caz de incidente cibernetice care să aibă drept bază planurile naționale de intervenție, cu care să se interconecteze. Acest plan ar trebui să furnizeze mecanismele și procedurile de bază pentru comunicarea dintre state membre și, nu mai puțin important, să sprijine amploarea și organizarea viitoarelor exerciții paneuropene. ENISA va colabora cu statele membre pentru a elabora, până în 2012, acest plan european de intervenție în caz de incidente cibernetice. În aceeași perioadă, toate statele membre vor elabora periodic planuri naționale de intervenție, precum și exerciții de

[42] A se vedea http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

[43] A se vedea http://www.enisa.europa.eu/.

reacție la incidente și redresare în urma acestora. FESM va fi responsabil de coordonarea necesară pentru obținerea acestor rezultate.

Ameliorarea colaborării dintre CERT naționale/guvernamentale

Realizări

– Colaborarea dintre CERT naționale/guvernamentale s-a intensificat. Activitatea ENISA legată de capacitățile de bază pentru CERT naționale/guvernamentale, de exercițiile CERT și exercițiile naționale, precum și de gestionarea incidentelor cibernetice a contribuit la stimularea și sprijinirea unei colaborări paneuropene mai strânse între CERT naționale/guvernamentale.

Etapele următoare

– ENISA va continua să sprijine colaborarea dintre CERT naționale/guvernamentale. În acest scop, ea va realiza în 2011 o analiză a cerințelor și va oferi orientări cu privire la un canal adecvat de comunicare sigură cu CERT, propunând inclusiv o foaie de parcurs pentru implementarea și evoluția viitoare a acestuia. De asemenea, ENISA va analiza lacunele operaționale la nivel european și va prezenta un raport privind modalitățile prin care se poate consolida colaborarea transfrontalieră dintre CERT și părțile interesate relevante, în special în ceea ce privește coordonarea pentru a reacționa la incidente.

– Agenda digitală pentru Europa invită statele membre să instituie **până în 2012** o rețea de CERT la nivel național care să funcționeze în mod corespunzător.

4. Cooperarea internațională

Reziliența și stabilitatea internetului

Realizări

– Principiile și orientările europene pentru reziliența și stabilitatea internetului[44] au fost elaborate pe baza lucrărilor realizate în cadrul FESM.

Etapele următoare

– În 2011, Comisia: va promova și va discuta aceste principii atât în cadrul colaborării bilaterale cu partenerii internaționali, în special SUA, cât și în dialogurile din cadrul G8, OCDE, Meridian și ITU; va iniția consultări cu părțile interesate relevante, în special din sectorul privat, la nivel european (prin EP3R) și internațional (prin forumul dedicat guvernanței internetului, *Governance Internet Forum*, și prin alte foruri adecvate); și va promova discuții cu actorii/organizațiile cheie de pe internet.

– În 2012, partenerii internaționali vor proceda la transformarea acestor principii și orientări într-un cadru comun propice angajamentului colectiv internațional privind reziliența și stabilitatea internetului pe termen lung.

[44] A se vedea http://ec.europa.eu/information_society/policy/nis/index_en.htm

Exerciții la nivel internațional privind redresarea și atenuarea incidentelor internet de mare amploare

Realizări

– Șapte state membre[45] au luat parte la exercițiul cibernetic al SUA, Cyber Storm III, în calitate de parteneri internaționali. Comisia și ENISA au participat ca observatori.

Etapele următoare

– În 2011, Comisia va elabora în colaborare cu SUA, în cadrul Grupului de lucru UE-SUA privind securitatea și infracționalitatea cibernetică, un program comun și o foaie de parcurs pentru realizarea de exerciții transcontinentale comune/sincronizate în 2012/2013. Totodată, vor fi avute în vedere opțiuni de includere și a altor regiuni sau țări care se confruntă cu probleme similare, în vederea punerii în comun a abordărilor și a activităților aferente.

5. Criterii pentru infrastructurile critice europene din sectorul TIC

Criterii specifice sectorului pentru identificarea infrastructurilor critice europene pentru sectorul TIC

Realizări

– Discuțiile tehnice din cadrul FESM privind criteriile specifice sectorului pentru TIC au dus la elaborarea unui proiect de criterii pentru comunicațiile fixe și mobile și internet.

Etapele următoare

– FESM va continua discuțiile tehnice privind criteriile specifice sectorului pentru TIC în vederea finalizării acestora până la sfârșitul anului 2011. În paralel, o serie de consultări cu sectorul privat cu privire la proiectul de criterii pentru sectorul TIC sunt avute în vedere de unele state membre și la nivel european, prin EP3R.

– Comisia va discuta cu statele membre elementele specifice sectorului TIC care trebuie avute în vedere pentru revizuirea Directivei 2008/114/CE privind identificarea și desemnarea infrastructurilor critice europene care va avea loc în 2012.

–

[45] FR, DE, HU, IT, NL, SE și UK.