COMISIA COMUNITĂȚILOR EUROPENE

Bruxelles, 30.3.2009
COM(2009) 149 final

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

privind protecția infrastructurilor critice de informație

„Protejarea Europei de atacuri cibernetice și perturbații de amploare: ameliorarea gradului de pregătire, a securității și a rezilienței”

{SEC(2009) 399}
{SEC(2009) 400}

(prezentată de Comisie)

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

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. INTRODUCERE

Tehnologiile informaţiei şi comunicaţiilor (TIC) sunt din ce în ce mai mult prezente în activităţile zilnice ale fiecăruia dintre noi. Parte din aceste sisteme, servicii, reţele şi infrastructuri TIC (pe scurt, infrastructuri TIC) reprezintă o latură esenţială a economiei şi societăţii europene, furnizând bunuri şi servicii vitale ori funcţionând drept platformă de sprijin pentru un număr de alte infrastructuri critice. Infrastructurile TIC sunt considerate infrastructuri critice de informaţie (ICI)[1], întrucât distrugerea sau perturbarea acestora ar avea un impact grav asupra unor funcţii societale vitale. Exemple recente ale unor astfel de situaţii includ atacurile cibernetice de amploare îndreptate împotriva Estoniei din 2007 şi ruperea cablurilor transcontinentale din 2008.

Forumul Economic Mondial estima, în 2008, că există o probabilitate cuprinsă 10 şi 20% de apariţie a unei distrugeri majore a ICI în următorii 10 ani, cu un cost economic global potenţial de aproximativ 250 miliarde USD[2].

Prezenta comunicare se concentrează pe prevenirea, gradul de pregătire şi pe conştientizarea riscurilor şi defineşte un plan de acţiuni imediate în scopul ameliorării securităţii şi rezilienţei ICI. Accentul pus pe aceste aspecte se înscrie în linia dezbaterii lansate la solicitarea Consiliului şi a Parlamentului European de a aborda provocările şi priorităţile unei politici privind securitatea reţelelor şi a informaţiilor (SRI), precum şi instrumentele cele mai potrivite pentru a face acest lucru la nivel european. Acţiunile propuse vin totodată în completarea celor care vizează prevenirea, combaterea şi urmărirea activităţilor criminale şi teroriste îndreptate împotriva ICI, aflându-se în sinergie cu eforturile de cercetare actuale şi planificate ale UE în domeniul securităţii reţelelor şi informaţiilor, precum şi cu iniţiativele internaţionale din acest domeniu.

2. CONTEXTUL STRATEGIC

Prezenta comunicare are drept obiectiv prezentarea politicii europene privind creşterea securităţii şi a nivelului de încredere în societatea informaţională. Încă din 2005, Comisia[3] a subliniat necesitatea urgentă de coordonare a eforturilor de construire a încrederii tuturor părţilor implicate în comunicaţiile electronice şi în serviciile din acest domeniu. În acest scop,

---

1 COM(2005) 576 final propune o definiţie a ICI.
2 *Global Risks 2008*
3 COM(2005) 229

în 2006 a fost adoptată o strategie pentru o societate informațională mai sigură[4]. Principalele elemente ale acesteia, printre care securitatea și reziliența infrastructurilor TIC, au fost confirmate în Rezoluția 2007/068/01 a Consiliului. Cu toate acestea, părțile implicate nu par să adere suficient la aceste imperative, iar gradul de implementare a strategiei ar putea fi crescut. La nivel tactic și operațional, strategia consolidează totodată rolul Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA), înființată în 2004 pentru a contribui la garantarea unui nivel ridicat și eficace de securitate a rețelelor și a informației în Comunitate și la dezvoltarea culturii securității rețelelor și a informației în beneficiul cetățenilor europeni, a consumatorilor, a întreprinderilor și a administrațiilor.

În 2008, mandatul ENISA a fost extins fără modificări până în martie 2012[5]. În același timp, Consiliul și Parlamentul European au făcut un apel pentru *„continuarea discuțiilor referitoare la viitorul ENISA și pentru orientarea generală a eforturilor europene către o securitate sporită a rețelelor și a informației."* În sprijinul acestei dezbateri, Comisia a lansat în noiembrie anul trecut o consultare publică on-line[6], ale cărei rezultate vor fi făcute publice în curând.

Activitățile prevăzute în prezenta comunicare se derulează în cadrul Programului european pentru protecția infrastructurii critice (PEPIC)[7] și în paralel cu acesta. Un element-cheie al PEPIC este Directiva[8] privind identificarea și clasarea infrastructurilor critice europene[9], care identifică TIC ca sector prioritar în viitor. Un alt element important al PEPIC este rețeaua de alertă privind infrastructurile critice (RAIC)[10].

În ceea ce privește aspectele normative, propunerea Comisiei de reformă a cadrului normativ pentru rețele și servicii de comunicații electronice[11] cuprinde prevederi noi privind securitatea și integritatea, în special în vederea accentuării obligațiilor operatorilor de a depune toate eforturile pentru luarea măsurilor corespunzătoare care să conducă la limitarea riscurilor, la garantarea continuității furnizării serviciilor și la notificarea breșelor de securitate[12]. Aceste procese converg înspre obiectivul general de ameliorare a securității și a rezilienței ICI. Parlamentul European și Consiliul manifestă un sprijin extins pentru aceste prevederi.

Acțiunile propuse în prezenta comunicare completează măsurile existente, precum și măsurile prevăzute în domeniul cooperării judiciare și polițienești îndreptate către prevenirea, combaterea și urmărirea activităților criminale și teroriste care vizează infrastructurile TIC, așa cum se prevede *inter alia* în Decizia-cadru a Consiliului privind atacurile asupra sistemelor informaționale[13], precum și în modificările previzionate ale acesteia[14].

Această inițiativă ia în considerare activitățile NATO privind politica comună în domeniul apărării împotriva criminalității cibernetice, i.e. Autoritatea de Management pentru Apărare

---

4 COM(2006) 251
5 Regulamentul (CE) nr. 1007/2008
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 final
8 2008/114/EC
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 COM(2008) 676 final
11 COM(2007) 697, COM(2007) 698, COM(2007) 699.
12 Articolul 13 din directiva-cadru
13 2005/222/JHA
14 COM(2008) 712

împotriva Criminalității Cibernetice și Centrul de Excelență pentru Apărare împotriva Criminalității Cibernetice.

Nu în ultimul rând, inițiativa ține seama și de evoluțiile internaționale în domeniu, în special de principiile G8 cu privire la protecția ICI[15], Rezoluția 58/199 a Adunării Generale a ONU privind *crearea unei culturi mondiale a securității cibernetice și protecția infrastructurilor critice de informație* și recenta recomandare a OECD privind protecția infrastructurilor critice de informație.

3. IMPLICAțII

3.1. Infrastructurile critice de informație sunt esențiale pentru creșterea economică și dezvoltarea societală a UE

Rolul economic și societal al sectorului TIC și al infrastructurilor TIC este subliniat într-o serie de rapoarte recente privind inovarea și creșterea economică. Printre acestea se numără Comunicarea privind evaluarea intermediară a i2010[16], raportul grupului Aho[17] și rapoartele economice anuale ale Uniunii Europene[18]. OECD subliniază importanța TIC și a internetului în ceea ce privește *„stimularea performanței economice și a bunăstării sociale și consolidarea capacității societăților de a ameliora calitatea vieții cetățenilor de pretutindeni"*[19]. Totodată, OECD recomandă politici care sporesc încrederea în infrastructurile internet.

Sectorul TIC este esențial pentru toate zonele societății. Întreprinderile se bazează pe sectorul TIC atât în ceea ce privește vânzările directe, cât și în privința eficienței proceselor interne. TIC reprezintă o componentă esențială a inovării și sunt răspunzătoare de aproximativ 40% din creșterea de productivitate[20], utilizarea acestora fiind de asemenea generalizată în activitatea administrațiilor publice locale și centrale: adoptarea serviciilor de e-guvernare la toate nivelurile, precum și noi aplicații, cum ar fi soluțiile inovatoare din domeniul sănătății, energiei și al participării politice fac ca sectorul public să fie puternic dependent de TIC. Nu în ultimul rând, cetățenii se bazează din ce în ce mai mult pe serviciile societății informaționale și utilizează TIC în activitățile zilnice: ameliorarea securității ICI are potențialul de a spori încrederea cetățenilor în TIC, printr-o mai bună protecție a datelor personale și a dreptului la viață privată, printre altele.

3.2. Riscurile cu care se confruntă infrastructurile critice de informație

Riscurile datorate atacurilor provocate de factorul uman, catastrofelor naturale și deficiențelor tehnice nu sunt întotdeauna pe deplin înțelese și/sau suficient analizate. Prin urmare, nivelul de sensibilizare al părților interesate este insuficient pentru elaborarea de măsuri de protecție și de contramăsuri adecvate.

Atacurile cibernetice au evoluat la un nivel de complexitate fără precedent. Experimente simple devin astăzi activități complexe desfășurate în scopul obținerii de profituri sau din

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
16 COM(2008) 199 final
17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
18 *EU Economy 2007 Review* http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
19 http://www.oecd.org/dataoecd/1/29/40821707.pdf
20 http://epp.eurostat.ec.europa.eu/ - Știință și tehnologie/Societatea informațională

raționamente politice. Atacurile cibernetice de amploare împotriva Estoniei, Lituaniei și Georgiei sunt cele mai mediatizate exemple ale unei tendințe generale. Numărul foarte mare de viruși, viermi și alte forme de malware, răspândirea botneturilor și creșterea continuă a numărului de spamuri confirmă gravitatea problemei[21].

Nivelul ridicat de dependență de ICI, interconectarea și interdependența transfrontalieră a acestora cu alte infrastructuri, precum și vulnerabilitățile și amenințările cu care se confruntă sporesc nevoia de abordare a problemei securității și rezilienței acestora dintr-o perspectivă sistemică, ca primă linie de apărare împotriva deficiențelor tehnice și a atacurilor.

3.3. Securitatea și reziliența infrastructurilor critice de informație poate spori încrederea în societatea informațională

Pentru a garanta utilizarea infrastructurilor TIC la întregul potențial și pentru a profita astfel de oportunitățile economice și sociale ale societății informaționale, toate părțile implicate trebuie să aibă un nivel ridicat de încredere în acestea. Acest lucru depinde de o multitudine de elemente, cel mai important fiind asigurarea unei securități și reziliențe ridicate. Diversitatea, deschiderea, interoperabilitatea, facilitatea utilizării, transparența, responsabilitatea și posibilitatea auditării diferitelor componente, precum și concurența reprezintă motoarele evoluțiilor în materie de securitate și stimulează conceperea de produse, procese și servicii de ameliorare a securității. Așa cum Comisia a subliniat deja[22], această responsabilitate este una comună: părțile implicate luate individual nu dispun de mijloacele necesare pentru a asigura securitatea și reziliența tuturor infrastructurilor TIC și de a îndeplini toate sarcinile pe care aceste deziderate le presupun.

Asumarea acestor responsabilități implică o abordare și o cultură din perspectiva managementului riscurilor, capabile să răspundă amenințărilor cunoscute și să anticipeze amenințările viitoare, fără a reacționa exagerat și fără a împiedica apariția de servicii și aplicații inovatoare.

3.4. Provocările pentru Europa

În completarea activităților legate de implementarea Directivei privind identificarea și clasarea infrastructurilor critice europene, în special identificarea criteriilor specifice pentru sectorul TIC, este necesară abordarea unor provocări de ordin mai general, care să contribuie la ameliorarea securității și rezilienței ICI.

3.4.1. Abordări la nivel național inegale și necoordonate

Cu toate că provocările și aspectele cu care se confruntă statele membre prezintă elemente comune, măsurile instituite de acestea în vederea asigurării securității și rezilienței ICI, precum și nivelul de pregătire și de expertiză sunt diferite.

Abordările la nivel pur național prezintă riscul de fragmentare și ineficiență la nivelul întregii Europe. Abordările naționale diferite și lipsa unei cooperări transfrontaliere sistematice reduc substanțial eficacitatea contramăsurilor luate de fiecare stat membru, *inter alia,* întrucât interconectarea ICI presupune că un nivel de securitate și de reziliență scăzut într-un stat membru are potențialul de a crește vulnerabilitatea și riscurile în celelalte.

---

[21] COM(2006) 688 final

[22] COM(2006) 251 final

Pentru a rezolva această situație, este necesar un efort la nivel european care să aducă valoare adăugată politicilor și programelor naționale prin creșterea gradului de sensibilizare și a unei înțelegeri pe baze comune a provocărilor; stimularea adoptării de obiective și priorități strategice comune; creșterea cooperării între statele membre și integrarea politicilor naționale într-o dimensiune orientată mai mult spre aspectele europene și internaționale.

3.4.2. Necesitatea unui model european de guvernanță pentru ICI

Ameliorarea securității și rezilienței infrastructurilor critice de informație ridică probleme speciale de guvernanță. În vreme ce statele membre rămân responsabile de definirea politicilor legate de ICI, implementarea acestora depinde de implicarea sectorului privat, care deține sau controlează un număr important de ICI. Pe de altă parte, piețele nu oferă întotdeauna suficiente stimulente pentru a încuraja sectorul privat să investească în protecția ICI la nivelul solicitat în mod obișnuit de sectorul public.

Pentru soluționarea acestei probleme, la nivel național au apărut parteneriatele public-privat (PPP), ca model de referință. Cu toate acestea, în ciuda unui consens asupra faptului că parteneriatele public-privat ar fi de dorit și la nivel european, acest lucru nu s-a materializat încă. Un cadru de guvernanță care să implice o serie de părți interesate la nivel european, care ar putea include și un rol sporit pentru ENISA, ar putea încuraja implicarea sectorului privat în definirea obiectivelor strategice de politică publică, precum și a priorităților și măsurilor operaționale. Acest cadru ar reprezenta puntea de legătură dintre politicile naționale și realitatea operațională de pe teren.

3.4.3. La nivel european, capacitate limitată de alertă rapidă și de reacție în caz de incidente

Mecanismele de guvernanță vor fi cu adevărat eficace numai în măsura în care toți participanții dispun de informații pertinente. Acest lucru este îndeosebi relevant pentru administrațiile centrale, care au responsabilitatea în ultimă instanță de a garanta securitatea și bunăstarea cetățenilor.

Cu toate acestea, procesele și practicile de monitorizare și de raportare a incidentelor de securitate a rețelelor diferă de la un stat membru la altul. Unele dintre acestea nu dispun de o organizație de referință ca punct de monitorizare. Un aspect și mai important este faptul că schimbul de date concrete privind incidentele de securitate și cooperarea dintre statele membre par insuficient dezvoltate, desfășurându-se pe baze informale sau limitându-se la schimburi bilaterale sau, în cazul schimburilor multilaterale, implicând un număr redus de state membre. În plus, exercițiile de simulare a incidentelor sau cele care testează capacitatea de reacție sunt esențiale pentru ameliorarea securității și rezilienței ICI, în special prin concentrarea pe strategii și procese flexibile de abordare a aspectelor neprevăzute ale potențialelor crize. La nivelul UE, exercițiile din domeniul securității cibernetice se află încă în stadiul embrionar. Exercițiile care depășesc frontierele naționale sunt foarte puține. Așa cum au demonstrat evenimentele recente[23], sprijinul reciproc reprezintă un element esențial în cadrul unei reacții adecvate la amenințările și atacurile de amploare la adresa ICI.

Un sistem european puternic de alertă rapidă și de reacție în caz de incidente trebuie să aibă la bază echipe naționale/guvernamentale de intervenție în caz de incidente de securitate în

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

domeniul IT (CERT) funcționale, așadar care să dispună de o bază comună în ceea ce privește capabilitățile. Aceste structuri trebuie să acționeze drept catalizatori la nivel național ai interesului părților implicate, precum și ai capacității acestora de a-și asuma activități care țin de politicile publice (inclusiv activități legate de sistemele de partajare a informațiilor și alertelor către cetățeni și IMM-uri) și să se angajeze într-o cooperare și un schimb de informații transfrontaliere eficace, eventual pe baza lecțiilor oferite de unele organizații existente, precum Grupul CERT Guvernamentale Europene[24].

3.4.4. Cooperarea internațională

Evoluția internetului ca și ICI cheie necesită acordarea unei atenții deosebite rezilienței și stabilității acestuia. Internetul, datorită structurii sale distribuite și redundante s-a dovedit a fi până acum o infrastructură foarte robustă. Evoluția spectaculoasă a acestuia a condus însă la o complexitate fizică și logică în creștere, precum și la apariția de noi servicii și utilizări: preocupările legate de capacitatea sa de a rezista în fața numărului din ce în ce mai mare de perturbări și de atacuri cibernetice sunt așadar legitime.

Diversitatea opiniilor cu privire la caracterul critic al elementelor care intră în componența internetului explică în parte diversitatea pozițiilor adoptate la nivel guvernamental exprimate în foruri internaționale, cât și percepțiile contradictorii asupra importanței acestui aspect. Acest lucru ar putea dăuna eficienței prevenirii, gradului de pregătire și capacității de redresare după incidente, care afectează internetul. Spre exemplu, consecințele tranziției de la IPv4 la IPv6 trebuie evaluate inclusiv în ceea ce privește securitatea ICI.

Internetul este o rețea de rețele globală și înalt distribuită, cu centre de control care nu urmează neapărat granițele naționale. Acest aspect impune o abordare specifică și orientată în vederea asigurării rezilienței și stabilității acestuia, bazată pe două măsuri convergente. Întâi, ajungerea la un consens asupra priorităților la nivel european privind reziliența și stabilitatea internetului, din punct de vedere al politicii publice și al implementării operaționale. În al doilea rând, implicarea comunității globale în elaborarea unui set de principii, care să oglindească valorile centrale europene, cu privire la reziliența și stabilitatea internetului, în contextul dialogului și cooperării strategice cu țările terțe și cu organizațiile internaționale. Aceste activități derivă din recunoașterea, de către Summitul Mondial privind Societatea Informațională[25], a importanței cruciale a stabilității internetului.

4. CALEA DE URMAT: CĂTRE COORDONARE ȘI COOPERARE SPORITE LA NIVELUL UE

Datorită dimensiunii comunitare și internaționale a problemei, o abordare integrată la nivelul UE pentru sporirea securității și rezilienței ICI ar completa și ar aduce valoare adăugată programelor naționale existente și schemelor de cooperare bilaterală și multilaterală dintre statele membre.

Discuțiile legate de politicile publice inițiate în urma evenimentelor din Estonia sugerează că efectele unor atacuri similare pot fi limitate prin măsuri preventive și prin acțiuni coordonate desfășurate în momentul crizei. Schimburile mai structurate de informații, precum și de bune practici la nivelul UE ar putea facilita în mod considerabil combaterea amenințărilor transfrontaliere.

---

[24] http://www.egc-group.org/

[25] Agenda Tunis pentru societatea informațională, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Este necesară consolidarea instrumentelor existente de cooperare, inclusiv a ENISA, precum și crearea de noi instrumente, dacă este cazul. De asemenea, este esențială o abordare care să implice o multitudine de părți interesate, la mai multe niveluri la scară europeană, în completarea responsabilităților naționale și cu respectarea deplină a acestora.

Este de asemenea necesară buna înțelegere a mediului de lucru și a constrângerilor impuse de acesta. De exemplu, natura distribuită a internetului, care permite utilizarea nodurilor de rețea drept vectori de atac, cum ar fi botneturile, reprezintă o preocupare. Totuși, natura distribuită reprezintă o componentă-cheie a stabilității și rezilienței și poate contribui la o redresare mai rapidă decât în cazul procedurilor supraformalizate, de sus în jos. Acest lucru necesită o analiză precaută de la caz la caz a politicilor publice și a procedurilor operaționale instituite.

Orizontul de timp este la rândul său important. Este în mod evident nevoie să acționăm acum și să creăm rapid elementele necesare pentru construirea unui cadru care să ne permită să răspundem provocărilor actuale, elemente care vor intra în componența viitoarei strategii pentru securitatea rețelelor și a informației.

Pentru abordarea acestor provocări, prezenta comunicare propune cinci piloni:

(1) Pregătire și prevenire: garantarea unui ridicat nivel de pregătire la toate nivelurile;

(2) Depistare și reacție: furnizarea de mecanisme adecvate de alertă rapidă;

(3) Redresarea după incidente și atenuarea acestora: întărirea mecanismelor UE de apărare a ICI;

(4) Cooperare internațională: promovarea pe plan internațional a priorităților UE;

(5) Criterii pentru sectorul TIC: sprijinirea implementării directivei privind identificarea și clasarea infrastructurilor critice europene[26].

5. PLANUL DE ACțIUNE

5.1. Pregătire și prevenire

Nivelul de bază comun de capabilități și servicii pentru cooperarea paneuropeană. Comisia invită statele membre și părțile implicate:

- să definească, cu sprijinul ENISA, un nivel minim de capabilități și servicii pentru CERT naționale/guvernamentale și operațiunile de intervenție în caz de incidente, în sprijinul cooperării paneuropene;
- să se asigure că CERT naționale/guvernamentale acționează ca și componentă-cheie a capacității naționale în materie de pregătire, schimb de informații, coordonare și reacție.

Obiectiv: sfârșitul anului 2010 pentru stabilirea standardelor minime; sfârșitul anului 2011 pentru instituirea în toate statele membre de CERT naționale/guvernamentale funcționale.

[26] Directiva 2008/114/CE a Consiliului

Parteneriatul public-privat european pentru reziliență (EP3R). Comisia

- va încuraja cooperarea dintre sectorul public și sectorul privat cu privire la obiectivele de securitate și reziliență, la cerințele de bază, la bunele măsuri și practici în materie de politică. Accentul principal al EP3R va fi pe dimensiunea europeană din perspectivă strategică (de exemplu bune practici în materie de politică) și tactică/operațională (de exemplu implementarea industrială). EP3R ar trebui să aibă la bază inițiativele naționale și activitățile operaționale existente ale ENISA și să vină în completarea acestora.

Obiectiv: sfârșitul anului 2009 pentru o foaie de parcurs și un plan pentru EP3R; mijlocul anului 2010 pentru instituirea de EP3R; sfârșitul anului 2010 pentru primele rezultate ale EP3R.

Forumul european pentru schimbul de informații între statele membre. Comisia

- va iniția un forum european pentru ca statele membre să poată face schimb de informații și bune practici de politică de securitate și rezistență a infrastructurilor critice de informație. Acesta va beneficia de pe urma rezultatelor activităților altor organizații, în principal ENISA.

Obiectiv: sfârșitul anului 2009 pentru lansarea forumului; sfârșitul anului 2010 pentru primele rezultate.

5.2. Depistare și reacție

Sistemul european de alertă și schimb de informații (EISAS). Comisia sprijină

dezvoltarea și implementarea EISAS, cu intenția de a extinde sistemul către cetățeni și IMM-uri și de a-l dezvolta pe baza sistemelor de alertă și de schimb de informații naționale și din mediul privat. Comisia sprijină financiar două proiecte de prototipuri complementare[27]. ENISA este invitată să facă inventarul rezultatelor acestor proiecte și al altor inițiative naționale și să producă o foaie de parcurs pentru continuarea dezvoltării și implementării EISAS.

Obiectiv: sfârșitul anului 2010 pentru finalizarea proiectelor de prototipuri; sfârșitul anului 2010 pentru foaia de parcurs referitoare la sistemul european.

5.3. Atenuarea riscurilor și redresarea după incidente

Planificarea pentru situații de urgență și exerciții la nivel național. Comisia invită statele membre:

- să elaboreze planuri naționale de urgență și să organizeze regulat exerciții de reacție în caz de incidente de securitate de amploare și de redresare după dezastru, în vederea ameliorării coordonării paneuropene. CERT/CSIRT naționale/guvernamentale pot primi sarcina de a organiza exerciții de planificare în caz de urgență și de test la nivel național, cu implicarea

[27] În contextul programului CE „Prevenirea, pregătirea și gestionarea consecințelor terorismului și ale altor riscuri referitoare la securitate” http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

părților interesate din sectorul public și din cel privat. ENISA este invitată să se implice în aceste acțiuni pentru a sprijini schimbul de bune practici între statele membre.

Obiectiv: sfârșitul anului 2010 pentru desfășurarea a cel puțin unui exercițiu la nivel național în fiecare stat membru.

Exerciții la nivel paneuropean de reacție în caz de incidente de securitate de mare amploare. Comisia

- va sprijini financiar dezvoltarea de exerciții paneuropene legate de incidente privind securitatea internetului[28], care pot constitui totodată platforma operațională pentru participarea paneuropeană la exerciții privind securitatea rețelelor la nivel internațional, cum ar fi Cyber Storm în Statele Unite.

Obiectiv: sfârșitul anului 2010 pentru conceperea și derularea primului exercițiu paneuropean; sfârșitul anului 2010 pentru participarea europeană la exerciții internaționale.

Ameliorarea colaborării dintre CERT naționale/guvernamentale. Comisia invită statele membre:

- să întărească cooperarea dintre CERT naționale/guvernamentale, printre altele prin utilizarea și extinderea mecanismelor de cooperare cum ar fi ECG (Grupul CERT naționale/guvernamentale)[29]. ENISA este invitată să joace un rol activ în stimularea și sprijinirea cooperării paneuropene dintre CERT naționale/guvernamentale, ceea ce va avea ca rezultat creșterea gradului de pregătire; consolidarea capacității europene de reacție și de răspuns în caz de incidente; exerciții la nivel paneuropean (și/sau regional).

Obiectiv: sfârșitul anului 2010 pentru dublarea numărului de organisme naționale participante în cadrul ECG; sfârșitul anului 2010 pentru elaborarea de către ENISA a materialelor de referință pentru sprijinirea cooperării paneuropene.

5.4. Cooperarea internațională

Reziliența și stabilitatea internetului. Sunt prevăzute trei activități complementare:

- Priorități europene privind reziliența și stabilitatea pe termen lung ale internetului. Comisia va anima o dezbatere la nivel european, cu implicarea părților interesate competente din sectorul public și privat, în vederea definirii priorităților UE în ceea ce privește reziliența și stabilitatea pe termen lung ale internetului.

Obiectiv: sfârșitul anului 2010 pentru prioritățile UE cu privire la componentele și aspectele critice legate de internet.

- Principii și linii orientative pentru reziliența și stabilitatea internetului (la nivel european). Comisia va colabora cu statele membre în scopul definirii liniilor orientative pentru reziliența și stabilitatea internetului, concentrându-se *inter alia* asupra acțiunilor de redresare la nivel regional, a acordurilor de asistență reciprocă, a strategiilor coordonate de

[28] *Supra* 27
[29] *Supra* 24

redresare și continuitate, a distribuției geografice a resurselor internet critice, a introducerii măsurilor de precauție tehnologice în arhitectura și protocoalele internet, a reproducerii și diversității datelor și serviciilor. Comisia finanțează deja un *task force* pentru reziliența DNS, ceea ce va contribui la atingerea unui consens, pe lângă alte proiecte din acest domeniu[30].

Obiectiv: sfârșitul anului 2009 pentru o foaie de parcurs la nivel european referitoare la principiile și liniile orientative pentru reziliența și stabilitatea internetului; sfârșitul anului 2010 pentru un acord privind proiectul de document conținând aceste principii și linii orientative.

- Principii și linii orientative pentru reziliența și stabilitatea internetului (la nivel global). Comisia va colabora cu statele membru în vederea elaborării unei foi de parcurs privind promovarea la nivel mondial a principiilor și a liniilor orientative. Se va dezvolta cooperarea strategică cu țări terțe, în special în contextul dialogurilor pe tema societății informaționale, ca vector de construire a unui consens la scară globală[31].

Obiectiv: începutul anului 2010 pentru o foaie de parcurs privind cooperarea internațională referitoare la principiile și liniile orientative pentru securitate și reziliență; sfârșitul anului 2010 pentru proiectul de document cuprinzând principiile și liniile orientative recunoscute la nivel internațional care urmează să fie discutate cu țări terțe și în forurile competente, inclusiv în Forumul privind guvernanța internetului.

Exerciții la nivel internațional privind redresarea și atenuarea incidentelor internet de mare amploare. Comisia invită părțile interesate europene:

- să reflecteze cu privire la o modalitate practică de a extinde la nivel global exercițiile derulate în contextul pilonului de redresare și atenuare a incidentelor, plecând de la planurile în caz de urgență și de la capabilitățile regionale.

Obiectiv: sfârșitul anului 2010 pentru propunerea de către Comisie a unui cadru și a unei foi de parcurs pentru sprijinirea implicării europene și pentru participarea europeană la exerciții la nivel global privind redresarea după incidente internet de mare amploare și atenuarea acestora.

5.5. Criterii pentru infrastructurile critice europene din sectorul TIC

Criterii specifice pentru sectorul TIC. Plecând de la experiența activității inițiale desfășurate în 2008, Comisia

- va continua să dezvolte, în cooperare cu statele membre și cu toate părțile implicate competente, criteriile pentru identificarea infrastructurilor critice europene din sectorul TIC. În acest scop, va fi lansat un studiu specific care va furniza informațiile pertinente necesare[32].

30 *Supra* 27
31 COM(2008) 588 final
32 *Supra* 27

Obiectiv: prima jumătate a anului 2010 pentru definirea de către Comisie a criteriilor pentru infrastructurile critice europene din sectorul TIC.

6. CONCLUZII

Securitatea și reziliența ICI reprezintă prima linie de apărare împotriva deficiențelor și a atacurilor. Ameliorarea acestora la nivelul Uniunii Europene este esențială pentru a profita pe deplin de beneficiile aduse de societatea informațională. Pentru atingerea acestui obiectiv ambițios, prezenta comunicare propune un plan de acțiune în vederea consolidării cooperării tactice și operaționale la nivel european. Succesul acestor acțiuni depinde de capacitatea lor de a profita de pe urma activităților din sectorul public și de a fi benefice acestora, de angajamentul și de participarea deplină a statelor membre, a instituțiilor europene și a tuturor părților implicate.

În acest scop, pe 27-28 aprilie 2009 va avea loc o conferință ministerială, în cadrul căreia inițiativele propuse vor fi discutate cu statele membre și unde acestea își vor exprima angajamentul în favoarea unui dialog cu privire la o politică europeană pentru securitatea rețelelor informatice mai modernă și mai puternică.

În cele din urmă, ameliorarea securității și a rezilienței ICI este un obiectiv pe termen lung, a cărui strategie și măsuri necesită evaluări regulate. În consecință, întrucât acest obiectiv este în sinergie cu dezbaterea generală privind viitorul politicii privind securitatea rețelelor și a informației în UE după 2012, Comisia va iniția, către finalul anului 2010, un exercițiu de inventariere care să evalueze prima etapă de acțiuni și să identifice și să propună măsurile suplimentare necesare.