

Avizul Comitetului Economic și Social European privind Comunicarea Comisiei către Parlamentul European, Consiliul, 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”

COM(2009) 149 final

(2010/C 255/18)

Raportor: **dl McDONOGH**

La 30 martie 2009, în conformitate cu articolul 262 din Tratatul de instituire a Comunității Europene, Comisia Europeană a hotărât să consulte Comitetul Economic și Social European cu privire la

„Comunicarea Comisiei către Parlamentul European, Consiliul, 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”

COM(2009) 149 final.

Secțiunea pentru transporturi, energie, infrastructură și societatea informațională, însărcinată cu pregătirea lucrărilor Comitetului pe această temă, și-a adoptat avizul la 12 noiembrie 2009. Raportor: dl McDONOGH.

În cea de-a 458-a sesiune plenară, care a avut loc la 16 și 17 decembrie 2009 (ședința din 16 decembrie 2009), Comitetul Economic și Social European a adoptat prezentul aviz cu 179 de voturi pentru, și 4 abțineri.

1. Concluzii și recomandări

1.1 Comitetul salută comunicarea Comisiei privind planul de acțiune pentru protecția infrastructurilor critice de informație (ICI) în Europa. Comitetul împărtășește îngrijorarea Comisiei cu privire la vulnerabilitatea Europei față de atacuri cibernetice, deficiențe tehnice, atacuri provocate de factorul uman și catastrofe naturale, precum și la uriașele pagube pe care acestea le-ar produce economiei și a bunăstării cetățenilor UE. Împărtășim constatarea Comisiei referitoare la necesitatea de a acționa urgent pentru a spori coordonarea și cooperarea UE în fața acestei probleme critice. Suntem, de asemenea, de acord cu Comisia în ceea ce privește necesitatea de a elabora rapid un cadru politic cuprinzător pentru protecția ICI.

1.2 Comitetul ia notă de concluziile Conferinței ministeriale a UE privind protecția infrastructurilor critice de informație (CIIP) și este îngrijorat de slaba pregătire a Europei de a face față atacurilor cibernetice pe scară largă sau perturbațiilor ICI, dat fiind că abordările din fiecare stat membru necesare protecției ICI sunt adesea inegale și insuficient coordonate. Se cunoaște modul în care evoluția internetului și lipsa unei reflecții la nivel sistemic în privința securității și rezilienței infrastructurilor de informație au dat naștere situației grave în care ne aflăm în prezent. Cu toate acestea, dat fiind că necesitatea de lua măsuri a fost, în sfârșit, formulată, Comitetul îndeamnă Comisia să acționeze cu hotărâre și fără întârziere pentru a aborda această problemă.

1.3 Comitetul sprijină planul de acțiune la nivel înalt cu cinci piloni prezentat în comunicare și felicită Comisia pentru munca

sa; este extrem de dificil să se elaboreze o abordare integrată, cu implicarea tuturor părților interesate și pe mai multe niveluri în vederea creșterii securității și rezilienței ICI - în special ținând seama de caracterul heteroclit al părților interesate și de complexitatea infrastructurilor europene de informație. Comitetul recunoaște, de asemenea, importanța asistenței și contribuției Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) pentru îndeplinirea obiectivelor acestei comunicări.

1.4 Comitetul observă că părțile interesate nu au făcut suficiente eforturi de punere în aplicare a Rezoluției Consiliului 2007/C 68/01 privind securitatea și reziliența infrastructurii TIC ⁽¹⁾. De dificultatea de a elabora politici eficiente de protecție a celor mai critice infrastructuri de informație din Europa profită cei care intenționează să atace ICI din motive politice sau financiare. De aceea, Comitetul îndeamnă Comisia să-și asume mai ferm rolul de lider, necesar pentru a asocia toate părțile interesate și pentru a pune în aplicare măsuri eficiente de protejare a Europei de posibilele amenințări la adresa infrastructurilor sale critice de informație. Comitetul nu crede că planul de acțiune prezentat în comunicare va produce rezultatele așteptate atâta timp cât responsabilitatea punerii în aplicare nu este încredințată unei autorități de reglementare corespunzătoare.

1.5 Comitetul atrage atenția Comisiei asupra avizelor anterioare ale CESE care au formulat observații cu privire la necesitatea unei societăți informaționale sigure, la preocupările referitoare la securitatea online și la protecția infrastructurilor critice.

⁽¹⁾ COM(2006) 251

2. Recomandări

2.1 Uniunea Europeană ar trebui să încredințeze unei autorități de reglementare corespunzătoare, din care să facă parte membri ai Agenției pentru Drepturi Fundamentale a Uniunii Europene, răspunderea de a pune în aplicare o protecție eficientă a infrastructurilor critice de informație din întreaga UE.

2.2 Toate statele membre ar trebui să-și dezvolte o strategie națională, o politică și un cadru de reglementare solid, procese holistice de gestionare a riscurilor la nivel național, precum și măsuri și mecanisme adecvate de pregătire. În acest sens, fiecare stat membru ar trebui să constituie o echipă guvernamentală de intervenție în caz de incidente de securitate în domeniul IT (CERT) și să o afilieze Grupului Guvernamental European al CERT (EGC-*European Governmental Emergency Response Teams Group*) ⁽²⁾.

2.3 Comisia trebuie să-și accelereze eforturile în vederea înființării Parteneriatului public-privat european pentru reziliență (EP3R) și să-l asocieze activităților Agenției Europene pentru Securitatea Rețelelor Informatic și a Datelor (ENISA) și Grupului Guvernamental European al CERT (EGC).

2.4 Politica privind protecția infrastructurilor critice de informație (CIIP) ar trebui să se inspire, la toate nivelurile sale, din cele mai bune practici în materie de gestionare a riscului. Costul potențial al deficiențelor în materie de securitate și de reziliență ar trebui să fie cuantificat și comunicat părților interesate răspunzătoare respective.

2.5 Trebuie impuse sancțiuni, inclusiv de natură financiară, părților interesate care nu-și îndeplinesc sarcinile care le revin în cadrul unei politici CIIP, într-o măsură proporțională cu deficiențele sistemului cauzate de neglijența acestora.

2.6 Responsabilitatea pentru securitatea și reziliența ICI trebuie să le revină în cea mai mare parte părților interesate importante – guvernelor, furnizorilor de infrastructură și de tehnologie; acestora nu trebuie să li se permită să-și eludeze responsabilitatea prin transferarea acestora asupra consumatorilor, fie ei întreprinderi sau cetățeni.

2.7 Securitatea și reziliența trebuie asigurate în mod obligatoriu la conceperea tuturor sistemelor de tehnologii ale informației și comunicării (TIC) puse în aplicare în UE. Încurajăm părțile interesate din sectorul privat al CIIP să continue să facă eforturi pentru îmbunătățirea situației, mai ales în domeniile legate de reziliență, cum ar fi gestionarea rețelelor, gestionarea riscurilor și continuitatea operațională.

2.7.1 Stabilirea de bune practici și de standarde și verificarea respectării acestora trebuie să constituie o componentă fundamentală a oricărei politici care vizează prevenirea deficiențelor, măsurile de intervenție în caz de urgență și redresarea ICI.

2.7.2 Trebuie să se acorde prioritate punerii în aplicare a tehnologiilor IPv6 (cel mai recent protocol pentru adresele internet) și DNSSEC (ansamblu de programe destinate creșterii securității gestionării internaționale a sistemului de nume de domenii internet) pe întreaga rețea internet din UE, ceea ce va duce la o securitate sporită pe internet.

2.8 Încurajăm părțile interesate, atât din sectorul public, cât și din cel privat, să colaboreze în mod regulat pentru a-și verifica gradul de pregătire și măsurile de intervenție în caz de urgență, prin intermediul unor exerciții. Acordăm întregul sprijin propunerilor cuprinse în Comunicarea Comisiei privind organizarea, până în anul 2010, a primului exercițiu paneuropean.

2.9 Trebuie încurajată crearea în Europa a unei industrii puternice în domeniul securității informatice, pentru a corespunde competențelor existente în industria americană din domeniu, care beneficiază de fonduri importante. Investițiile în cercetarea și dezvoltarea pe teme legate de CIIP trebuie să crească substanțial.

2.10 Trebuie majorate fondurile consacrate dezvoltării de competențe și programelor de informare și de sensibilizare din domeniul securității cibernetice.

2.11 Trebuie înființate, în fiecare stat membru, agenții de informare și de asistență pentru a ajuta IMM-urile și cetățenii să înțeleagă care le sunt responsabilitățile în cadrul unei politici CIIP și pentru a se conforma acestora.

2.12 În interesul securității, UE ar trebui să-și dezvolte poziția privind viitorul guvernării internetului ⁽³⁾, care solicită o abordare cu caracter multilateral mai marcat, care să respecte prioritățile naționale ale SUA, reflectând totodată interesele Uniunii Europene. Acțiunea UE în acest domeniu ar trebui să includă o reflecție aprofundată asupra interacțiunilor dintre securitatea cibernetică și respectarea libertăților publice și private.

3. Context

3.1 Amenințarea unor atacuri cibernetice de amploare asupra infrastructurilor critice de informație

3.1.1 Infrastructurile critice de informație (ICI) cuprind tehnologiile informației și comunicării (TIC), care asigură platformele fundamentale de informație și comunicare pe baza cărora sunt furnizate bunuri și servicii fundamentale, inclusiv funcții societale vitale, cum ar fi aprovizionarea cu electricitate și apă, serviciile de transport, bancare, de sănătate și de urgență.

3.1.2 ICI sunt caracterizate de un nivel înalt de integrare a unor sisteme complexe, de interdependență în raport cu alte infrastructuri (de exemplu, cea de energie electrică), precum și de interconectarea transfrontalieră. Aceste infrastructuri sofisticate sunt astfel expuse unui mare număr de riscuri, care ar putea da naștere unor deficiențe ale sistemelor cu consecințe catastrofale, afectând simultan serviciile societale vitale în numeroase state membre. Riscurile ar putea proveni din erori umane, deficiențe tehnice, atacuri provocate de factorul uman (inclusiv de natură criminală sau din motive politice) și catastrofe naturale. Analiza riscurilor evidențiază lacunele unor astfel de sisteme, relevând totodată posibilitatea ca aceste sisteme să fie controlate prin practici care – intenționat sau nu – aduc atingere atât libertăților publice, cât și celor private. Comisia are obligația de a asigura respectarea drepturilor fundamentale în elaborarea legislației comunitare.

(2) <http://www.egc-group.org>

(3) COM(2009) 277 final.

3.1.3 Guvernele și ansamblul furnizorilor de servicii vitale nu fac cunoscute publicului deficiențele de securitate și reziliență decât dacă sunt obligați să o facă. Chiar și în aceste condiții, se cunosc numeroase exemple de amenințări la adresa infrastructurii critice cauzate de deficiențele de securitate și de reziliență de la nivelul ICI:

- în 2007 și 2008, au avut loc atacuri cibernetice de amploare în Estonia, Lituania și Georgia;
- în 2008, întreruperea cablurilor submarine intercontinentale din Mediterana și din Golful Persic a afectat traficul internet în numeroase țări;
- în aprilie 2009, responsabilii federali cu securitatea din SUA au avertizat cu privire la pătrunderea în rețeaua electrică a SUA a unor „spioni cibernetici”, în urma cărora au rămas în rețea programe informatice care ar putea fi folosite pentru a perturba sistemul;
- în luna iulie, SUA și Coreea de Nord au fost nevoite să facă față unor întreruperi manifeste ale serviciilor (implicând preluarea controlului asupra unui număr de 100 000-200 000 de calculatoare, devenite „zombi”), ceea ce a afectat funcționarea a numeroase site-uri guvernamentale.

3.1.4 Problema este exacerbată în mare măsură de intențiile distructive ale grupurilor criminale și de utilizarea războaielor cibernetice în scopuri politice.

- Prin exploatarea lacunelor sistemelor de operare ale calculatoarelor personale conectate la internet, grupurile criminale au creat așa-numitele *botnets* – rețele de calculatoare conectate prin intermediul unor programe de malware (*malicious software*) sub forma unui computer virtual unic care ascultă de comenzile răufăcătorilor („zombi” sau „drone”). Aceste *botnets* sunt folosite pentru diverse activități criminale și pentru a sprijini atacuri cibernetice de amploare conduse de teroriști și de guvernele implicate în războaie cibernetice, care închiriază de la criminali aceste *botnets* pentru a le folosi la rândul lor. Se estimează că una dintre aceste *botnets*, numită „Conficker” are la dispoziție mai mult de 5 milioane de PC-uri.

3.1.5 Costurile economice ale deficiențelor de ICI ar putea fi extrem de ridicate. Forumul Economic Mondial evaluează la 10-20 % probabilitatea de a înregistra în următorii 10 ani o avarie majoră la nivelul ICI, costul potențial la nivel global fiind de 250 de miliarde de dolari și mii de vieți omenești.

3.2 Problemele privind pregătirea pentru situații de urgență, securitatea și reziliența

3.2.1 Internetul reprezintă principala platformă pe care se bazează majoritatea ICI din Europa. Arhitectura internetului are la bază interconectarea a milioane de calculatoare, fabricația, comunicațiile și controlul acestora fiind distribuite în întreaga lume. Această arhitectură fragmentată este esențială pentru ca internetul să dea dovadă de stabilitate și reziliență, cu posibilitatea de a restabili rapid traficul în cazul în care apare o problemă. Aceasta înseamnă, însă, că atacurile cibernetice de amploare pot fi inițiate de la extremitățile rețelei, de exemplu prin intermediul *botnets*, de către orice răufăcător care are motivația și cunoștințele de bază necesare.

3.2.2 Rețelele globale de comunicare și ICI presupun un nivel înalt de interconectivitate transfrontalieră. În aceste condiții, nivelul scăzut de securitate și de reziliență a rețelei dintr-o țară poate afecta negativ securitatea și reziliența ICI în toate celelalte țări cu care este interconectată. Dată fiind această interdependență la nivel internațional, Uniunii Europene îi revine sarcina de a elabora o politică integrată de gestionare a securității ICI și a rezilienței pe întreg teritoriul UE.

3.2.3 Nivelul de cunoștințe și de conștientizare a riscurilor care amenință ICI este scăzut, atât în rândul celor mai multe părți interesate, cât și în numeroase state membre. Foarte puține țări dispun de o politică globală de gestionare a acestor riscuri.

3.2.4 Propunerile de reformă privind cadrul de reglementare comun pentru rețelele și serviciile de comunicații electronice vor întări obligația operatorilor de rețea de a lua măsuri adecvate pentru identificarea riscurilor, asigurarea continuității serviciilor și comunicarea incidentelor de încălcare a securității (⁴).

3.2.5 Marea majoritate a tehnologiilor care stau la baza platformei pentru ICI este furnizată de sectorul privat, iar asigurarea unei cooperări adecvate în vederea garantării unei protecții eficiente a ICI depinde în mare măsură de existența unui nivel ridicat de competență, încredere, transparență și comunicare între toate părțile interesate – guverne, întreprinderi și consumatori.

3.2.6 Este fundamental să se recurgă la o abordare internațională pe mai multe niveluri, care să implice toate părțile interesate.

3.3 Planul de acțiune cu cinci piloni

Comisia propune un plan de acțiune cu cinci piloni pentru a aborda aceste provocări:

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. Atenuarea riscurilor și redresarea după incidente: 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 (⁵).

(⁴) Articolele 13a și 13b din COM(2007) 697 final, referitoare la propunerile de amendamente la Directiva 2002/21/CE.

(⁵) Directiva Consiliului 2008/114/CE

În cadrul fiecărui pilon sunt stabilite obiective specifice cu termene de îndeplinire, unele dintre acestea mergând până la sfârșitul anului 2011.

4. Observații

4.1 Va fi extrem de dificil să se elaboreze și să se pună în aplicare o strategie eficientă pentru protecția ICI prin abordarea pe bază consultativă, voluntară și de cooperare prezentată în comunicarea Comisiei. Având în vedere gravitatea problemei și caracterul său urgent, Comitetul recomandă Comisiei să analizeze politica urmată în Marea Britanie și în SUA, și anume investirea unui autorități de reglementare cu responsabilitatea și puterea legală necesare în acest sens.

4.2 Comitetul este de acord cu îndemnul Rezoluției 58/199 a Adunării Generale a ONU privind crearea unei culturi mondiale a securității cibernetice și protecția infrastructurilor critice de informație. Având în vedere că, în ceea ce privește securitatea și reziliența ICI, țările depind unele de altele - „puterea unui lanț este egală cu cea a verigii celei mai slabe” - este îngrijorător faptul că numai 9 state membre au creat echipe CERT până în prezent și s-au alăturat grupului EGC. Constituirea acestor echipe trebuie să devină prioritară în cadrul agendei interguvernamentale.

4.3 Printre părțile interesate din domeniul securității cibernetice a UE se numără orice cetățean a cărui viață ar putea să depindă de serviciile esențiale. Cetățenii sunt, de asemenea, răspunzători de protecția conexiunii lor la internet împotriva atacurilor, în măsura propriilor posibilități. O răspundere și mai mare revine furnizorilor de tehnologie și servicii din TIC care fac posibilă utilizarea ICI. Este esențial ca toate părțile interesate să fie informate în mod corespunzător cu privire la securitatea cibernetică. Pentru Europa, este important, de asemenea, să se dispună de un mare număr de experți în domeniul securității și a rezilienței TIC.

4.4 Comitetul recomandă ca, în fiecare stat membru, să existe o organizație al cărei rol să fie acela de a informa, conștientiza și sprijini sectorul IMM-urilor pe teme legate de securitatea cibernetică. Companiile mari pot dobândi cu ușurință cunoștințele necesare, însă IMM-urile au nevoie de sprijin.

4.5 Dat fiind că sectorul privat este cel care furnizează cea mai mare parte a ICI, este important să se încurajeze un grad înalt de încredere și cooperare cu ansamblul întreprinderilor responsabile pentru ICI. Inițiativa EP3R, lansată de Comisie în luna iunie, merită salutăată și încurajată. Cu toate acestea, Comitetul consideră că această inițiativă trebuie sprijinită printr-o legislație care să impună cooperarea celor părți interesate care nu se implică în mod responsabil.

4.6 Rațiunea de a fi a gestionării riscurilor ca disciplină științifică este aceea de a facilita rezolvarea problemelor de tipul celor conținute în prezentul document. Comisia ar trebui să insiste în

planul său de acțiune asupra utilizării, după caz, a celor mai bune practici din domeniul gestionării riscurilor. Trebuie subliniată în mod deosebit utilitatea cuantificării riscurilor și costurilor unor eventuale deficiențe, pentru fiecare nivel al ICI. Atunci când probabilitatea și costul posibil al unor deficiențe sunt cunoscute, părțile interesate pot fi motivate mai ușor să treacă la acțiune. Este, de asemenea, facilitată tragerea lor la răspundere pe plan financiar pentru neîndeplinirea obligațiilor care le revin.

4.7 Părțile interesate importante încearcă să-și restrângă responsabilitatea folosindu-se de puterea lor de pe piață pentru a-i obliga pe clienți sau pe furnizori să accepte condiții care protejează întreprinderea mare în raport cu propria responsabilitate, de exemplu prin acorduri de licență pentru programe informatice sau acorduri de interconectare ISP care limitează răspunderea în cazul unor incidente legate de securitate. Aceste acorduri ar trebui să fie considerate ilegale, iar răspunderea ar trebui să revină întreprinderii mari.

4.8 Securitatea și reziliența pot și trebuie să fie incorporate în conceperea fiecărei rețele TIC. Prioritatea ar trebui să fie analiza topologiei arhitecturii rețelei în statele membre și în UE în ansamblu, pentru a identifica punctele în care se înregistrează o concentrare inacceptabil de mare a fluxului de informații și cele care prezintă un risc ridicat de deficiență a rețelei. În special marea concentrare a traficului internet într-un număr extrem de redus de IXP (*Internet Exchange Points*) în anumite state membre constituie un risc inacceptabil.

4.9 Comitetul invită, de asemenea, Comisia să consulte observațiile formulate anterior cu privire la COM(2008) 313 final - „Promovarea progresului internetului - Plan de acțiune privind implementarea versiunii 6 a protocolului Internet (IPv6) în Europa” ⁽⁶⁾. Recomandăm, de asemenea, punerea în aplicare, în măsura posibilului, a tehnologiilor DNSSEC, pentru a spori securitatea internetului.

4.10 Odată cu lansarea politicii sale privind securitatea cibernetică, SUA au preconizat pentru 2009 și 2010 cheltuieli bugetare de 40 de miliarde de dolari în acest domeniu. Aceasta reprezintă o infuzie masivă de fonduri în sectorul securității și va face ca numeroase întreprinderi din domeniul securității tehnologiilor informatice, inclusiv întreprinderi din Europa, să-și concentreze eforturile în SUA. De asemenea, întreprinderile americane din domeniul securității vor fi astfel încurajate să devină lideri la nivel mondial. Este de preferat ca Europa să dispună de propria ei industrie ultramodernă, care să concureze de pe poziții egale cu întreprinderile americane și ca industria din domeniul securității să investească suficiente eforturi și să se concentreze asupra necesităților europene în materie de infrastructură. Comitetul solicită Comisiei să reflecteze asupra unei posibile căi de a contrabalansa acest stimulent financiar masiv oferit de SUA.

⁽⁶⁾ JO C 175, 28.7.2009, p. 92.

4.11 Comitetul susține recenta comunicare a Comisiei privind viitorul guvernării internetului ⁽⁷⁾. În opinia Comitetului, UE trebuie să exercite o influență sporită asupra practicilor și politicilor ICANN (*Internet Corporation for Assigned Names and Numbers* – societatea care atribuie nume de domenii și numere în cadrul

internetului) și IANA (*Internet Assigned Numbers Authority* – autoritatea însărcinată cu atribuirea numerelor adreselor internet), iar actuala supraveghere unilaterală exercitată de către SUA ar trebui înlocuită cu mecanisme care să instituie o responsabilitate internațională și multilaterală.

Bruxelles, 16 decembrie 2009

Președintele
Comitetului Economic și Social European
Mario SEPI

⁽⁷⁾ COM(2009) 277 final.