

Analiză de risc și de vulnerabilitate pentru infrastructurile critice ale societății informatice – societate a cunoașterii

*Adrian V. Gheorghe**

1. Problematika vulnerabilității și riscului în Societatea Informatică – Societatea Cunoașterii

Societatea românească se află în mijlocul unor profunde transformări politice, economice, sociale și culturale. Acest ansamblu de transformări afectează viața fiecăruia dintre noi.

Societatea Informatică – Societatea Cunoașterii va depinde cu siguranță de performanțele infrastructurilor critice ale economiei românești ex. sistemele de producere, transport și distribuție ale energiei, sistemele de telecomunicație, bănci, sistemele de transport aerian, naval, pe cale ferată și pe cale rutieră, care vor putea fi tot mai mult accesate din interiorul granițelor naționale, dar și din afara acestora.

Societatea informatică – societatea cunoașterii redefiniște problematica și doctrina de apărare națională; aspectele economice nu vor fi cele doar strict legate de business și / sau de afaceri. Securitatea infrastructurilor critice ale societății românești vor trebui asigurate la un înalt nivel de complexitate, înțelegere și acțiune.

“Cunoașterea”, ca atare, va deveni o “armă” de apărare împotriva riscurilor, ale noilor vulnerabilități ce vor apare cu siguranță în societatea deceniilor viitoare. Prin *vulnerabilitate* se înțelege identificarea unui ansamblu de evenimente externe sistemelor tehnice care pun în pericol existența infrastructurilor tehnice, ale sistemelor informatice, cu precădere, și reprezintă elemente de inițiere în cadrul analizelor de risc specializate, cu luarea în considerare a probabilităților apariției elementelor de hazard și consecințele negative ale propagării dezastrelor. Ceea ce se numesc astăzi tot mai des pericole cibernetice (cyberthreats) vor deveni mai prezente în etapele noi de tranziție către o societate informatică – societate a cunoașterii.

La sfârșitul anilor '80, un diplomat român în una din țările nordice declară cu mândrie patriotică: “scoate din priză calculatoarele din societatea occidentală și aceasta va fi pierdută. Noi (românii) nu avem nevoie de o societate informatică, pentru a fi așadar vulnerabili”.

În etapa nouă politică, economică și culturală în care se află România, este evident că lucrurile s-au inversat. Un diplomat român astăzi va afirma cu siguranță că “fără a fi cuplată la Internet, fără o cultură informatică minimă, societatea românească, întreaga ei structură economico-politică și culturală nu va mai fi nicidecum și nicidecum compatibilă cu noile structuri euro-atlantice”.

* Universitatea Politehnică București, Swiss federal Institute of Technology (ETH), Zürich, Switzerland. E-mail: adrian.gheorghe@switzerland.org

Este, așadar, numai o chestiune de timp când se fac afirmații de un tip sau altul?

2. Teze ale vulnerabilității și riscurile infrastructurilor critice în societatea informațională – societatea cunoașterii

Cunoașterea, și managementul acesteia, au devenit resursa principală a societăților moderne actuale. Firme de mare reputație internațională, înainte cu câțiva ani erau producătoare de echipamente energetice de mare performanță ca de exemplu firma elvețiano-suedeză ABB, sau firma Sultzer. Astăzi ele se declară *knowledge management companies* (companii care procesează, coordonează și conduc o micro economie bazată pe cunoștințe).

Schimbările așteptate în viitor, de la o societate bazată eminentemente pe resurse materiale la o societate a utilizării resurselor inteligente care se profilează deja astăzi, conduce la integrarea pe scară largă a prelucrării și managementul cunoștințelor și a informației. Aceasta este o schimbare structurală în condițiile de globalizare, acces la Internet, etc.

În lucrarea de față mă voi rezuma la vulnerabilitatea infrastructurilor critice în condițiile adoptării unei noi doctrine politice de dezvoltare în România, cea a societății informatice, a societății cunoașterii.

În terminologia adoptată recent, infrastructurile critice sunt definite prin:

- Structurile informatice și de comunicație
- Băncile și sistemul financiar ale unei țări
- Sistemele de energie, incluzând cele de producere și transport ale electricității, ale petrolului și ale gazului natural
- Structuri de distribuție fizică ale resurselor ex.: sistemele de transport feroviare, rutiere, navale, aeriene
- Serviciile vitale suport ale activităților umane (sanitare, apărarea civilă, poliția, armata).

Vulnerabilitatea acestor sectoare, în condițiile accentuării introducerii în managementul societății, a informaticii și cunoașterii (information and knowledge) trebuie re-evaluată și considerată în toată amplitudinea ei.

Avantajul României este acela că va proiecta și realiza aceste infrastructuri suport ale prelucrării și managementul informațiilor în condiții în care deja alte societăți (societatea occidentală) se confruntă deja cu definirea și managementul riscurilor specifice; aceasta are loc pe măsura asimilării de noi structuri tehnice care implică o complexitate generalizată a tehnologiei, rețelelor, sistemelor tehnologice suport. Căderea, pentru numai o oră, a sistemului de calculatoare ale bursei din New York - SUA, a creat în iunie 2001 panică și confuzie mondială.

România, ca viitor partener în structurile economice globale și euro – atlantice, va trebui cu precădere să-și definească o strategie suport de identificare a vulnerabilităților și minimizarea riscurilor infrastructurilor ei critice.

3. Soluții posibile

În perspectiva accentuării, în România, a introducerii și promovării elementelor societății informatice - societatea cunoașterii, o serie de aspecte noi trebuie identificate și controlate:

- Crescândă dependență față de infrastructurile critice ale societății: în perspectivă, dependența fiecăruia dintre noi va fi tot mai mare față de sistemele de producere, distribuție și transport ale energiei electrice, sistemele de comunicație și a sistemelor de calculatoare
- Va avea loc o creștere a vulnerabilității sistemelor infrastructurilor critice în etapele de trecere accentuată în România la societatea informatică - societatea cunoașterii:
 - Se vor diversifica posibilitățile de provocare a unor daune clasice (ex.: riscurile tehnologice provocate de sisteme active (centrale nucleare-electrice, chimice) sau de sisteme tehnice așa numite pasive (ex. baraje ale centralelor hidroelectrice)
 - Vor apare noi pericole de tip și natură cibernetică: extinderea rețelelor de calculatoare, accesul la un computer personal (PC) și o conexiune telefonică clasică poate provoca intenționat daune însemnate
 - Complexitatea sistemelor tehnice și a interdependențelor acestora, precum și posibila / probabila interacțiune cu catastrofele naturale vor reprezenta noi elemente de vulnerabilitate pentru infrastructurile critice ale societății.

Spectrul pericolelor se va extinde și poate, în principiu, să includă:

- Evenimente naturale și accidente tehnice ce pot provoca daune materiale, ecologice și umane importante;
- Erori umane și omisiuni, care prin suportul fizic al societății informatice – societatea cunoașterii, poate induce efecte transversale negative în numeroasele componente ale infrastructurilor critice.

O eroare umană provocată în sistemul de distribuție a energiei electrice, induce nealimentarea cu energie a sistemului de transport feroviar privind transportul substanțelor periculoase.

Hackerii, cei care din numeroase motive personale sau sociale, aflați pe teritoriul României sau în afara acesteia, pot provoca intenționat discontinuități grave ale funcționării infrastructurii informatice ale viitoarei societăți informatice - societate a cunoașterii:

- *Activități criminale*
- *Spionaj industrial*

- *Terorism*
- *Război informatic.*

Ceea ce reprezintă astăzi vulnerabilitate și risc pentru societățile occidentale avansate, ele vor reprezenta elemente de input negativ și stres pentru societatea românească, ca societate informatică – societate a cunoștințelor. Bunăoară, trebuie depuse de la început eforturi pentru cunoașterea, localizarea și minimizarea încă de la început a efectelor potențial negative ce pot apare în societatea informatică – societate a cunoașterii, infrastructurile critice ale societății.

În etapa actuală de proiectare a structurilor societății informatice – societate a cunoașterii, trebuie accentuate următoarele aspecte:

- *Crearea unei culturi de securitate (safety culture)* la nivelul publicului, specialiștilor, managerilor și politicienilor. Noi legi trebuie adoptate și promovate pe măsură ce societatea informatică – societate a cunoașterii demarează ca un proces continuu și ireversibil;
- *Asigurarea unor infrastructuri manageriale* corespunzătoare, diseminate la toate nivelurile și adaptate gradual la necesitățile societale;
- *Elaborarea unui sistem de legi specifice* protecției infrastructurilor critice, în consens cu legislația internațională și Europeană;
- *Elaborarea unui program de cercetare științifică și dezvoltare* care să asigure progresul în *cunoașterea și managementul complexității* și interacțiunilor în cadrul infrastructurilor critice ale societății informatice – societatea cunoașterii.

Necesitatea creării unui program de conștientizare și de educație pentru a face față cerințelor generate de promovarea societății informatice – societatea cunoașterii este un alt aspect ce trebuie considerat cu atenție. În acest sens, este de remarcat faptul că promovarea societății informatice – societatea cunoașterii presupune un amplu program de educare, de înțelegere a dimensiunilor promovării procesului de a naviga continuu spre realizarea acestor deziderate ale societății informatice – societate a cunoașterii.

Industria privată sau cea cu participare publică are sarcina de a coopera și de a schimba informații în vederea asigurării funcționalității, în condiții de maximă securitate a infrastructurilor critice.

În orice societate, dar cu precădere în societatea informatică - societate a cunoașterii, infrastructurile critice pot fi caracterizate ca acelea care asigură "*linia vieții*" (lifelines infrastructures), de care societatea contemporană este astăzi pe deplin dependentă.

În societatea informatică – societatea cunoașterii nu mai există frontiere, în sensul clasic al acestei accepțiuni. Infrastructurile critice, linii ale vieții, sunt expuse la noi tipuri de vulnerabilitate – *vulnerabilități cibernetice* – și noi pericole, *pericole cibernetice*.

Modul de abordare al vulnerabilităților și riscurilor societății informatice – societate a cunoașterii, trebuie să adopte noile dimensiuni cibernetice specifice acestora. Acestea sunt deja concluzii pe care și le-au asumat și recente studii cu rezonanță în SUA și Europa Occidentală. Se menționează în aceste studii că "ceea ce este extrem de

important este de a recunoaște că atât deținătorii cât și cei ce operează infrastructurile informatice sunt astăzi în prima linie în ceea ce privește efortul pentru asigurarea securității acestora. Aceștia sunt, în primul rând, cei mai vulnerabili la atacurile cibernetice. Și această vulnerabilitate are influențe negative asupra securității naționale, competitivitatea economică globală și a bunăstării la nivel național.”

Societatea informatică - societatea cunoașterii implică adoptarea și negocierea unei noi geografii informatice, în care granițele sunt irelevante și distanțele geografice fără sens, unde inamicul potențial poate “demola” sistemele vitale ale societății fără nici un act de prezență sau agresiune așa numită militară.

Pe măsură ce vom face eforturi pentru a atinge scopurile și avantajele societății informatice - societatea cunoașterii, în paralel trebuie să avem în vedere că trebuie proiectate structuri și rețele de conducere în societatea informatică – societatea cunoașterii *reziliente*, capabile să răspundă noii geografii a vulnerabilității și riscurilor infrastructurilor critice din România.

Înainte de a atinge stadiile societății informatice – societății cunoașterii, România va trebui să gospodărească inteligent și eficace ansamblul infrastructurilor critice existente, cu vârsta lor tehnologică, gradul lor de întreținere. Aceasta nu este o iluzie sau o simplă ipoteză de lucru, ci un deziderat extrem de serios și din perspectiva în care forma de proprietate a acestora suferă profunde schimbări. Apoi integrarea dinamică a infrastructurilor existente cu cele specifice societății informatice – societatea cunoașterii va presupune recunoașterea și managementul unor vulnerabilități specifice.

Analizele de risc și vulnerabilitate pentru aceste categorii de sisteme, evoluția lor în etape de tranziție, ținând cont de gradul de educație și pregătire pentru managementul sistemelor complexe, vor avea un rol extrem de important în deceniul viitor.

O concluzie posibilă în etapa de demarare a dezideratelor societății informatice – societatea cunoașterii este aceea că analiza de vulnerabilitate și risc trebuie considerate cu precădere.

Se afirma recent că “...a aștepta apariția dezastrelor este o strategie periculoasă. Acum este timpul pentru a acționa în vederea protejării viitorului nostru”.

În noua geografie a riscurilor generate de existența infrastructurilor critice în cadrul societății informatice – societatea cunoașterii este necesar să învățăm să gândim diferit asupra operabilității conceptelor de vulnerabilitate, siguranță, securitate și risc.

Referitor la definirea direcțiilor de construcție și coordonare a eforturilor societale pentru societatea informatică – societatea cunoașterii, o serie de aspecte se vor evidenția în continuare:

- Se impune cu necesitate schimbul reciproc de informații, date și cunoștințe referitor la vulnerabilitatea diferitelor sisteme de infrastructuri critice, între Guvern și sectoarele implicate, transversal între sectoare distincte în cadrul conceptului de infrastructuri critice, în condițiile societății informatice – societatea cunoașterii

- Este necesar să se construiască în cadrul societății informatice – societatea cunoașterii, un sistem de responsabilități care să garanteze cooperarea între diferitele grupuri active în funcționarea infrastructurilor critice
- Protecția infrastructurilor impune construirea de capacități integrate în cadrul diverselor instituții în structura generală a societății în România
- Este necesară realizarea unei *culturi de securitate* (safety culture) corespunzătoare
- Sistemul de legi ale societății informatice – societatea cunoașterii trebuie să ia în considerare potențialul de impact al pericolelor cibernetice și reglementate în mod corespunzător
- Se impune inițierea și coordonarea adecvată a unor activități de cercetare științifică care să adreseze problematica vulnerabilității și securității infrastructurilor critice în cadrul conceptului de societate informatică – societatea cunoașterii.

În legătură cu realizarea unor studii practice care să adreseze problematica vulnerabilității și riscului infrastructurilor critice se impune, ca în condițiile României, să se:

- Promoveze construirea unor *bănci de date* care să colecteze și prelucreze date specifice infrastructurilor critice
- Construirea de *bănci de cunoștințe* care să înglobeze cea mai bună practică (best practice) privind proiectarea și funcționarea infrastructurilor critice în lume și în România, în special
- Promovarea unor *programe de învățământ* la nivel universitar și postuniversitar pentru a face față nevoilor specifice analizei vulnerabilității și riscului infrastructurilor critice ale societății informatice – societatea cunoașterii din România
- Instituirea în cadrul *structurii Academiei Române* a unui grup de lucru, comisie sau task force, pentru o activitate de cercetare interdisciplinară pe problematica vulnerabilității și riscului sistemelor complexe, în special al infrastructurilor critice și impactul lor la nivel național
- Se va impune cu siguranță adoptarea unei *terminologii unitare* în acest domeniu
- Realizarea unui *parteneriat* la nivel național între domeniul public și cel privat care să asigure un nivel acceptabil al securității infrastructurilor critice în cadrul societății informatice – societatea cunoașterii, fără să afecteze operabilitatea funcțiilor vitale ale economiei naționale din România
- Promovarea în toate etapele ciclului de viață al infrastructurilor critice ale societății informatice – societatea cunoașterii a *studiilor și analizei de risc*, promovând cea mai bună practică (best practice) și adoptarea unor criterii de risc cu largă acceptabilitate societală (ex. principiul *ALARA* –As Low As Reasonable Acceptable)
- Coordonarea în cadrul *sistemului de legi* din România a introducerii unor prevederi care să conducă la descurajarea atacurilor critice asupra infrastructurilor critice, dar și includerea de elemente legislative care să încurajeze soluții de tip risc-beneficiu privind proiectarea, realizarea și funcționarea operativă a infrastructurilor critice, în condițiile creșterii complexității și a dependabilităților acestora

- Promovarea, susținerea și realizarea în practică a unui ansamblu de măsuri specifice creării unei conștientizări a acțiunilor în caz de urgență (emergency awareness) care împreună cu cele ale culturii de securitate (safety culture) să depășească *momentele posibile de criză* în funcționarea infrastructurilor critice ale societății informatice – societatea cunoașterii
- Realizarea unor schimburi de informații și experiență internațională prin crearea și de societăți/fundații în România care să disemineze cea mai bună practică privind asigurarea continuității operabilității infrastructurilor critice (ex. Fundația *Infosurance*¹ în Elveția).

4. Concluzii

În loc de concluzii, se pot lua în considerare următoarele remarci, în scopul unor analize mai aprofundate și realizarea unui *business plan* referitor la promovarea și implementarea principiilor societății informatice – societatea cunoașterii:

Remarca 1: Managementul riscurilor societății informatice – societatea cunoașterii necesită, în general, un *parteneriat dedicat între industrie, Guvern, societate*.

Remarca 2: Structurile de decizie ale societății românești trebuie să fie construite pe principiul de *adaptabilitate și răspuns la crize* privind disfuncționalitatea infrastructurilor critice.

Remarca 3: Se impune, în perspectiva construirii cu intensitate a cadrului și dimensiunilor societății informatice – societatea cunoașterii, luarea în considerare a *pericolelor cibernetice* (cyberthreats) și anticiparea și mărginirea adecvată a efectelor acestora la niveluri diferite ale societății.

Remarca 4: Adoptarea conceptelor “*cash and carry security*” sau “*buy-in security*” vor deveni instrumentale în cadrul structurilor economiei de piață pentru România.

Aplicarea lor va genera forme noi de promovare durabilă a elementelor concrete ale societății informatice – societatea cunoașterii.

Referințe bibliografice

- [1] Critical Foundations. Protecting America’s Infrastructures. The Report of the President’s Commission on Critical Infrastructure Protection, Washington DC, October 1997
[2] Infosurance, Zürich, 2001.

¹ Infosurance realizează un sistem complex de activități privind posibila vulnerabilitate a sistemelor informatice la scara societății elvețiene