INFRASTRUCTURI INFORMAȚIONALE CRITICE

Lt.col.drd. Mirela BĂDEANA
Mr.ing.drd. Sorin FLOREA

"A Critical Infrastructure (CI) represents a subsystem of which disfunctionalities or destruction can have a deeply negative impact on national security and both social and economic wellfare. One nation's key sectors (informatics and communications, finance and banks, energy, logistics, medical services, defence, police) –CIs- depend, a large measure, on the interdependency of certain inter/national software and control systems. This information infrastructure (called Critical Information Infrastructure - CII) deals with the permanent and changing interactions with the knowledge-based societies, where it opens systems, CI monitoring and control, mass media and ICT converge.

The paper tries to differentiate some CI and CII aspects, following some major lines: sectorial, interdependencies, risk and system analyses and threats, vulnerabilities, impact evaluations.

In the end, some examples from main countries give the practical view on the CI and CII concepts, and an international frame is sketched."

Societatea informațională integrează obiectivele dezvoltării durabile, bazată pe dreptate socială şi egalitate a şanselor, protecție ecologică, libertate, diversitate culturală şi dezvoltare inovativă, restructurarea industriei şi a mediului de afaceri şi reprezintă o nouă etapă a civilizației umane care permite accesul larg la informație, un nou mod de lucru şi de cunoaştere, şi va amplifica posibilitatea globalizării economice şi a creşterii coeziunii sociale. Suportul tehnologic al noii societăți se constituie prin convergența a trei sectoare: tehnologia informației, tehnologia comunicațiilor, producția de conținut digital.

Societatea informatică este o societate a cunoaşterii şi depinde cu siguranță de performanțele infrastructurilor critice ale economiei româneşti, de exemplu sistemele de producere, transport şi distribuție ale energiei, sistemele de telecomunicație, băncile, sistemele de transport aerian, naval, pe cale ferată şi pe cale rutieră, care vor putea fi tot mai mult accesate din interiorul granițelor naționale, dar şi din afara acestora.

Societatea informatică, ca societate a cunoaşterii, redefineşte problematica şi doctrina de apărare națională; aspectele economice nu vor fi cele doar strict legate de business şi/sau de afaceri. Securitatea infrastructurilor critice ale societății româneşti va trebui asigurată la un înalt nivel de complexitate, înțelegere şi acțiune.

"Cunoaşterea", 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, şi reprezintă elemente de inițiere în cadrul analizelor de risc specializate, cu luarea în considerare a probabilităților apariției elementelor de hazard şi 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 cunoaşterii.

Generalități

Cunoaşterea şi 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 şi conduc o microeconomie bazata pe cunoştințe).

Schimbările aşteptate în viitor, de la o societate bazată eminamente pe resurse materiale la o societate a utilizării resurselor inteligente care se profilează deja astăzi, conduce la integrarea pe scară largă a prelucrării şi a managementului cunoştințelor şi a informației. Aceasta este o schimbare structurală în condițiile de globalizare, acces la Internet etc.

În terminologia adoptată recent, infrastructurile critice sunt definite prin:

- structurile informatice şi de comunicație;
- băncile şi sistemul financiar ale unei țări;
- sistemele de energie, incluzând cele de producere şi de transport ale electricității, ale petrolului şi ale gazului natural;
- structurile de distribuție fizică ale resurselor, de exemplu: 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 şi cunoaşterii (*information and knowledge*) trebuie reevaluată şi considerată în toată amplitudinea ei.

Sectoarele (zonele) cheie ale societății moderne, inclusiv cele vitale pentru securitatea națională şi pentru funcționarea esențială a economiei,

industriei depind de un spectru de interdependență ridicată între software-ul de nivel național şi internațional, şi sistemele de control, pentru operarea continuă, fără întreruperi.

Această infrastructură de informații stă la baza multor elemente ale infrastructurii critice (CI) şi de aici, rezultă şi denumirea *infrastructură de informații critice* (CII). CII face un continuu schimb între noi tipuri de interacțiune cu societățile, fiind evidentă folosirea tot mai mare a sistemelor deschise pentru monitorizarea şi controlul operațiilor CI, precum şi convergența mass-media, a tehnologiei informației şi a comunicațiilor către informații şi comunicații integrate (ICT).

Creşterea valorii informației şi disponibilitatea mijloacelor electronice pentru prelucrarea unui volum din ce în ce mai mare de informații, nu fac din informații şi sistemele de informații doar bunuri fără preț, ci şi importante ținte. Deşi oportunitățile ICT sunt bine ştiute şi exploatate, consecințele legăturii CI cu CII nu sunt suficient înțelese. Sistemele de informații sunt expuse defecțiunilor, sunt ținte atractive pentru atacuri răuvoitoare şi sunt susceptibile la efectele distructive în cascadă. Aceste noi tipuri de riscuri şi de vulnerabilități au devenit o problemă de securitate majoră la nivel mondial.

Ca subiect de cercetare, un număr de aspecte (probleme) indică o nevoie urgentă de a asigura o protecție continuă a CII. Aceste aspecte se referă la:

- legăturile în CI;
- consecințele interdependențelor între diferitele subsisteme ale CI;
- posibilele efecte distructive în cascadă ale defecțiunilor;
- noile situații de urgență cu apariția unor noi vulnerabilități insuficient înțelese.

În ultimii ani, multe țări au făcut paşi către o mai bună înțelegere a vulnerabilităților şi amenințărilor ce afectează CII şi au întocmit planuri cu soluții posibile pentru protecția acestor bunuri critice (protecția infrastructurii de informații critice, CIIP).

Este de dorit (dar foarte greu de obținut) să se facă o distincție între cei doi termeni CIP (protecția infrastructurii critice) şi CIIP (protecția infrastructurii de informații critice).

În publicațiile oficiale, cei doi termeni sunt folosiți inconsistent. De cele mai multe ori rămâne neclar dacă articolele de specialitate se referă la CIP sau CIIP, din moment ce ambele concepte sunt, în mod frecvent schimbate într-o manieră nesistematică.

Mai curând, folosirea în paralel a celor doi termeni reflectă stadiul discuțiilor politice dintre țările care au abordat aceste probleme.

Oricum, există cel puțin o caracteristică pentru a face distincția între cele două concepte. În timp ce CIP cuprinde toate sectoarele critice ale infrastructurii unei țări, CIIP este doar o componentă a protecției detaliate, care se orientează către infrastructura informațiilor critice.

Evoluția studiilor privind protecția infrastructurilor informaționale critice

Infrastructura critică este percepută ca fiind o infrastructură sau un subsistem ale cărui disfuncționalități sau distrugere (parțială sau totală, intenționată sau nu) pot avea un impact negativ semnificativ asupra securității naționale, sau mai sugestiv, asupra bunăstării naționale economice şi/sau sociale.

Comisia prezidențială privind Protecția Infrastructurii Critice (PCCIP, B. Clinton, 1977) a făcut delimitarea între infrastructurile critice şi infrastructurile informaționale critice.

Infrastructurile informaționale critice pot avea mai multe modalități de abordare astfel:

- perspectiva tehnică, la nivel sistemic;
- perspectiva mediului de afaceri;
- perspectiva securității naționale;
- perspectiva legislativă.

Principalele concepte de bază utilizate sunt:

a) "termenul critic":
   - concept sistemic;
   - concept simbolic.

b) conceptul de infrastructură critică.

c) analiza pe țări:
   - definirea sectoarelor critice;
   - politici şi inițiative naționale CIIP;
   - structuri organizaționale implicate.
   - abordarea problemei privind avertizarea timpurie.

Fiecare țară îşi stabileşte propriile sectoare critice, de exemplu:

Franța are stabilite ca sectoare critice: sectorul bancar şi financiar; industria chimică şi biotehnologică; energia şi electricitatea; stațiile de energie nucleară; sănătatea publică; siguranța şi ordinea publică; telecomunicațiile; sistemele de transport; aprovizionarea cu apă şi agențiile publice:

• *Secretariatul General al Apărării (SGDN)* se ocupă de problemele de securitate națională şi internațională şi este subordonat direct primului ministru.

• *Direcția Centrală pentru Securitatea Sistemelor Informatice (DCSSI)* asigură consultanță guvernului francez, sprijină autoritatea națională de reglementare şi serviciile publice din domeniul securității sistemelor informatice. Realizează expertiza tehnică şi ştiințifică în acest domeniu, evaluează amenințările şi emite măsuri, în caz de alertă.

• *Biroul Central pentru Combaterea Criminalității din Domeniul Tehnologiei Înalte*

- *Parteneriatele private-publice*
- Comisia Consultativă Strategică pe probleme IT (CSTI)
- Institutul Francez de Securitate (ISDF)

De asemenea, are stabilite la nivel național următoarele structuri de avertizare timpurie:

- CERT: CERT-RENAR, CERTA şi CERT-IST
- CLUSIF (Clubul de securitate a Sistemelor Informatice Franceze
- Secretariatul General al Apărării Naționale (SGDN)

Statele Unite ale Americii are ca *sectoare critice stabilite***:** agricultura şi industria alimentară**;** sistemul bancar şi financiar**;** materialele chimice şi inflamabile**;** baza industrială a apărării; serviciile de urgență**;** sistemul energetic**;** educația superioară**;** sistemul de asigurări**;** aplicarea legii**;** produsele petroliere şi combustibilii**;** serviciile poştale şi de transport; sănătatea publică**;** telecomunicațiile şi tehnologia informației**;** transporturile şi protecție majoră pentru: bunuri comerciale cheie; baraje, diguri; locațiile guvernamentale**;** monumente şi simbolurile naționale**;** centrale nucleare.

Guvernul SUA consideră infrastructura informațională critică ca un element al strategiei sale de securitate națională şi promovează activ cooperarea şi înființarea unui parteneriat între sectorul public şi cel privat în acest domeniu.

Încă din anul 1990 au existat preocupări privind protecția infrastructurii critice în SUA, dar în urma evenimentelor din 11 septembrie 2001 fondurile şi mijloacele umane şi materiale implicate în această activitate au sporit substanțial. Au fost luate măsuri pentru identificarea şi asigurarea protecției infrastructurilor critice, transmiterea avertismentelor în timp util şi au fost emise reglementări pentru vehicularea informațiilor din infrastructura critică.

Instituțiile publice cheie din cadrul protecției infrastructurilor informaționale critice sunt:

- Direcția pentru Analiza Informațiilor şi Protecția Infrastructurii (IAIP);
- Comisia Prezidențială pentru Protecția Infrastructurii Critice (PCCIP);
- Departamentul pentru Securitatea Internă (DHS);
- Direcția pentru Analiza Informațiilor şi Protecția Infrastructurii (IAIP);
- Divizia Națională pentru Securitatea Cibernetică (NCSD);
- Oficiul de Asigurare a CI (CIAO);
- Centrul pentru Protecția Infrastructurii Naționale (NICP);
- Biroul pentru Securitatea Internă;
- Departamentul de Stat al SUA;
- Comunitatea de apărare;
- Secretarul Asistent pentru Securitatea Națională.

Directivele prezidențiale în sprijinul protecției infrastructurilor informaționale critice sunt:

- Directivele 62 şi 63 privind Decizia Prezidențială (PDD);
- Directiva Prezidențială privind Securitatea Internă/HDSP-7;
- Planul Național pentru Protecția Sistemelor Informatice;
- Deciziile Executive privind Securitatea Țării;
- Strategia Națională pentru Securizarea Spațiului Cibernetic (NSSC);
- Strategia Națională pentru Protecția Fizică a Infrastructurii Critice şi a Bunurilor Cheie.
- Procedurile privind vehicularea Informațiilor din Infrastructura Critică.

Parteneriatul public-privat:

- Oficiul de legătură cu Sectorul privat, Departamentul pentru Securitatea Internă;
- Infragardul;
- Alianța Națională pentru Securitate Cibernetică (NCSA).
- Parteneriatul privind Securitatea Structurii Critice (PCIS).

Structurile naționale pentru avertizarea timpurie:

- Biroul Federal de Investigații;
- Direcția pentru Analiza Informațiilor şi Protecția Infrastructurii (IAIP);
- US-CERT;
- FedCIRC;
- Centrul de coordonare CERT/CC;
- Alianța pentru Securitatea Internetului;
- Centrele pentru Partajarea şi Analizarea Informațiilor (ISAC).

Tipurile de analize şi evaluări în domeniul infrastructuri critice /infrastructuri informaționale critice:

- Analiza sectorială;
- Analiza interdependențelor;
- Analiza de risc;
- Evaluarea amenințărilor;
- Evaluarea vulnerabilităților;
- Evaluarea impactului;
- Analiza de sistem.

Analiza sectorială - Sector – un grup de industrii sau infrastructuri care îndeplinesc funcții similare

Canada – criterii pentru definirea criticalității – impactul în următoarele direcții:

- fără pierderi de vieți omeneşti;
- îndeplinirea cerințelor de bază ale comunității;

- continuitatea în afaceri;
- menținerea încrederii în guvern.

Olanda – etape ale programului BVI pentru protecția CI:

- analiza succintă a infrastructurilor critice olandeze;
- stimularea parteneriatului public-privat;
- analiza amenințărilor şi vulnerabilităților;
- analiza măsurilor de protecție.

Un produs sau un serviciu este considerat vital (foarte important) dacă are o contribuție esențială, în societate, în menținerea unui nivel calitativ considerat minimal al:

- ordinii şi legislației naționale şi internaționale;
- siguranței publice;
- economiei;
- sănătății publice;
- mediului ecologic.

Determinarea caracteristicilor specifice ale sectoarelor critice. Modele:

- Australia: PreDict
- Canada: CIPTF
- Germania: BSI
- Olanda: Bitbreuk şi KWINT
- Elveția: Roundtables
- SUA: DOE

Germania

ACIS – Analysis of Critical Infrastructure Sectors:

- examinarea sectoarelor potențial critice;
- examinarea proceselor relevante/sector;
- determinarea situațiilor care pot conduce la întreruperea proceselor;
- determinarea probabilităților de apariție a întreruperilor.

Categorii şi scale:

- efectele posibile ale daunelor: (nesemnificativ, minor, moderat, major, catastrofal);
- probabilitățile de apariție: (puțin probabil, improbabil, posibil, probabil, virtual sigur).

Analiza interdependențelor

Un concept recent este considerat aproape model universal pentru analiza interdependențelor. El descrie şase dimensiuni:

- mediul;
- comportamentul de răspuns;
- caracteristicile de infrastructură;

- tipurile de interdependențe;
- starea de operativitate;
- tipul de erori/defecte;
- modele de prezentare a analizei interdependențelor: matricea de dependență, RALS – Relational Analysis For Linked Systems.

Analiza de risc – probabilitatea ca o sursă de amenințare dată să producă o anumită vulnerabilitate potențială şi impactul care are loc asupra acelui eveniment (proces). Analiza sensului cuprinde identificarea, analizarea şi cuantificarea acestuia, conform celor 3 întrebări clasice:

a. Ce distrugeri/daune pot avea loc?

b. Care este probabilitatea apariției acestora?

c. Ce consecințe pot realiza?

Fazele de evaluare a riscului sunt:

a. Ce poate fi făcut?

b. Care opțiuni sunt disponibile şi care sunt efectele lor, în termeni de cost, beneficii şi risc?

c. Ce impact au deciziile managementului curent asupra evoluției viitoare a sistemului?

Paşii incluşi în analiza de risc în IT:

1. caracterizarea sistemului;
2. identificarea amenințărilor;
3. identificarea vulnerabilităților;
4. analiza controlului;
5. determinarea probabilităților;
6. analiza impactului sau a efectelor negative;
7. determinarea riscului.

Metode cunoscute:

Australia şi Noua Zeelandă: NSW
Canada: CIPTF
UE: CORAS
Franța: EBIOS
Norvegia: BAS
Elveția: Roundtable
Anglia: NISCC
SUA: OCTAVE

Proiectul CORAS (IST – 2000 – UB31)

Inițiere – 2001
Actualizare – 2003

Componente:

- terminologie;
- limbaj pentru modelare sisteme;
- proceduri de dezvoltare sisteme;
- management risc;
- metodologie pentru management risc;
- suport fizic rețele de calculatoare şi comunicații;
- etape identificare context, identificare risc, evaluare şi analiză risc, tratare risc;
- funcționare paralelă a două subprocese, comunicare şi consultare, monitorizare şi analiză.

Analiza amenințărilor

Amenințare – o entitate internă sau externă a sistemului având atât capabilitatea de a exploata vulnerabilitățile infrastructurilor critice, cât şi intenția de reducere a capacităților economice şi de apărare. Pot fi de natură: umană, naturală sau de mediu.

Exemple de sisteme de evaluare:

- Australia: MSW
- Canada: OCIPEP
- SUA: MIST

Tipuri de amenințări:

- naturale: inundații, cutremure, tornade, alunecări de teren;
- umane: atacuri de rețea, soft malițios, acces neautorizat;
- de mediu: poluare.

Sursele de amenințare pot fi: naturale, umane şi de mediu.

Sursele umane de amenințare sunt reprezentate de: hackeri, spărgători de parole, falsificarea identității; criminalitatea informatică, distrugerea informațiilor; dezvăluirea ilegală a informațiilor; câştigurile financiare; distrugerea neautorizată a datelor criminalitatea informatică (de exemplu urmărirea cibernetică); actele frauduloase; mituirea; înşelăciunea; intruziunea sistemului; şantajul terorist; distrugerea; exploatarea; răzbunarea; atacurile cu bombe/terorism; războiul informațiilor; atacurile asupra sistemului (negarea, refuzul serviciilor); penetrarea sistemului; încercarea de pătrundere în sistem; spionajul industrial (companii, guverne străine, interesele altor guverne); avantajul competitiv; spionajul economic; exploatarea economică; furtul de informații; pătrunderea în intimitatea personală (violarea intimității); ingineria

socială; penetrarea sistemului; accesul neautorizat la sistem (acces la informații clasificate, proprietate personală sau tehnologice); persoanele din interior (angajați slab pregătiți, nemulțumiți, neglijenți, necinstiți, cărora li s-a terminat contractul de muncă); curiozitatea; ego; inteligența; câştigurile financiare; erorile sau omisiunile neintenționate (de ex. introduceri eronate de date, erori de programare); actele de violență, atacurile asupra angajaților; browsingul informațiilor proprietate; abuzul informatic; frauda şi furtul; introducerea de date falsificate, corupte; interceptarea; codurile nocive (viruşi, bombe logice, cai troieni); vânzarea informațiilor personale; microfoanele secrete; sabotajul asupra sistemului;

Analiza vulnerabilităților

Vulnerabilitatea – caracteristică de proiectare, implementare şi/sau operare CI care induce printr-o amenințare distrugerea sau incapacitatea funcțională a sistemului.

Instrumente standardizate:

- Australia: Predict
- Germania: CYTEX
- Olanda: KWIMT
- SUA: DOE şi CIAO

Sistemul CIAO. Principalii paşi sunt:

1. MEI – Definirea Infrastructurii Esențiale Minime.
2. Colectarea de date pentru identificarea vulnerabilităților.
3. Analiza şi prioritizarea vulnerabilităților:

- fiecare vulnerabilitate este examinată pentru a vedea dacă aceasta are impact asupra uneia sau mai multor MEI;
- vulnerabilitățile sunt sortate după impactul asupra proceselor de bază;
- se generează un segment grafic al vulnerabilităților corespunzătoare procesului de bază;
- se face o analiză a probabilității ca vulnerabilitățile să fie exploatate luând în calcul amenințările potențiale la adresa agenției.

Evaluarea impactului

- *Evaluarea cantitativă*

- avantaj: furnizează o măsură cantitativă a impactului, care poate fi o intrare într-o analiză de tip "cost-beneficiu";
- dezavantaj: fiind o expresie numerică, este mai puțin clară, fiind necesară o interpretare suplimentară, în manieră calitativă;

• *Evaluarea calitativă*

- avantaj: prioritizează riscurile şi identifică zonele de intervenție imediată;
- dezavantaj: ieşirile analizei nefiind cuantificate, o analiză cost-beneficiu nu este posibilă.

Exemple:

• Canada: OCIPEP
• Anglia: NISE

Analiza de sistem

Nivele ierarhice:

• sistem de sisteme;
• infrastructuri individuale;
• sistem individual sau firma;
• componente tehnice.

Exemple de sisteme ABMS (Agent-based Modelling and Simulation):

• ACIP – model propus de UE. Determină ce fel de protecție a CI poate fi analizată şi evaluată prin modelare şi simulare. Produce o foaie de parcurs pentru:

- identificarea şi evaluarea stării CIP-ului;
- analiza dependențelor mutuale interinfrastructuri;
- efectul de avalanşă la perturbații;
- scanare pentru a determina goluri, deficiențe şi posibile perturbări;
- identificarea unor dezvoltări tehnologice şi a măsurilor de protecție.

• COSIM – aparține tot UE, are şase noduri în cinci țări. Scopul proiectului este să dezvolte o serie de mecanisme teoretice, grafice, analitice şi computaționale pentru descrierea comportării în rețea, pentru creştere şi evoluție, pentru transpunerea acestora în sisteme sociale şi economice.

• DepAuDe - aparține UE. Are ca obiectiv dezvoltarea unei metodologii şi arhitecturi pentru îmbunătățirea dependențelor sistemelor automate nesigure, critice, distribuite şi/sau înlănțuite;

• Safeguard – aparține UE şi se ocupă de dependența şi supraviețuirea infrastructurilor critice Complexe (CCCI).

• NISAC – este de origine SUA. A fost dezvoltat de laboratoarele de specialitate de la SANDIA şi Los Alamos. În esență obiectivul următor este de a prognoza, în timp real, consecințele întreruperilor din infrastructurile naționale critice.

Organizații internaționale:

NATO

• Ghidul ministerial pentru planificarea situațiilor de urgență civile (CEP).
• Comitetul de planificare a comunicațiilor civile (CCPC).

Documente publicate:

xxvii. Protecţia infrastructurilor critice în telecomunicaţii.

xxviii. Consecinţele întreruperii funcţionării infrastructurii critice în serviciile poştale.

xxix. Noile riscuri şi ameninţări în telecomunicaţiile civile.

xxx. Cerinţele CEP pentru coordonarea măsurilor de reglementare în telecomunicaţiile naţionale.

xxxi. Noi riscuri şi ameninţări pentru serviciile poştale.

CCPC a introdus în Planul de Acţiune al NATO pentru Apărarea Cibernetică următoarele documente:

xxxii. Consecinţele introducerii Forţei de reacţie rapidă în cazul situaţiilor de urgenţă în domeniul calculatoarelor.

xxxiii. Identificarea şi evaluarea interdependenţelor altor infrastructuri critice asupra reţelelor de comunicaţii civile.

xxxiv. Impactul şi oportunităţile pentru CEP NATO în dezvoltarea societăţii informatice.

Structurile NATO cu atribuţii în domeniu:

- Comitetul de Protecţie Civilă (CPC).
- Comitetul de Planificare Industrială (IPC).
- Comitetul pentru Planificare Alimentaţie şi Agricultură (FAPC).
- Comitetul de Planificare pentru Aviaţia Civilă (CAPC).
- Comisia de Planificare pentru Transportul Terestru (PBIST).
- Comisia de Planificare pentru Transportul Oceanic (PBOS).

UE

- impactul asupra cetăţeniei, educaţiei, afacerilor, sănătăţii şi comunicaţiilor.
- Planul de acţiune eEurope, cercetările în domeniul societăţii informatice, eContent, eSafety, Planul de acţiune pentru Internet.
- Programul "eEurope – o societate informatică pentru toţi" – a fost lansat de UE la 8 decembrie 1999 şi a fost adoptat în iunie 2002.
- În iunie 2001, Comisia Europeană a publicat o comunicare intitulată "Reţeaua şi Securitatea Informaţiei: Propunere pentru Abordarea Politicii Europene.
- La 11 februarie 2003, Comisia Europeană a prezentat o propunere pentru înfiinţarea "Agenţiei Europene pentru Reţea şi Securitatea Informaţiei – ENISA".

Problemele curente în legi şi legislație

La nivel internațional:

• Convenția Consiliului European pentru Criminalitatea Cibernetică – cel mai important instrument legislativ în domeniu.

- Facilitarea investigațiilor în domeniul criminalității informatice – un pas important fiind "Decizia Cadru privind Atacurile împotriva sistemelor Informatice" – redactată de Comisia Europeană, în aprilie 2002.

• Proiectul "Instrumente cibernetice pentru căutarea on-line a probelor" (CTOSE) – prevede standarde judiciare pentru pedepsirea crimelor cibernetice.

Avantajul României este acela că va proiecta şi va realiza aceste infrastructuri suport ale prelucrării şi managementul informațiilor în condiții în care alte societăți (societatea occidentală) se confruntă deja cu definirea şi cu 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 şi confuzie mondială.

În perspectiva accentuării, în România, a introducerii şi promovării elementelor societății informatice – societatea cunoaşterii, o serie de aspecte noi trebuie identificate şi controlate:

• Dependență crescândă față de infrastructurile critice ale societății: în perspectivă, dependența fiecăruia dintre noi va fi tot mai mare față de sistemele de producere, distribuție şi transport ale energiei electrice, sistemele de comunicație şi a sistemelor de calculatoare;

• Va avea loc o creştere a vulnerabilității sistemelor infrastructurilor critice în etapele de trecere accentuată, în România, la societatea informatică – societatea cunoaşterii;

• 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 aşa numite pasive (ex. baraje ale centralelor hidroelectrice);

• Vor apare noi pericole de tip şi natură cibernetică: extinderea rețelelor de calculatoare, accesul la un computer personal (PC) şi o conexiune telefonică clasică poate provoca intenționat daune însemnate;

• Complexitatea sistemelor tehnice şi a interdependențelor acestora, precum şi posibila/probabila interacțiune cu catastrofele naturale vor reprezenta noi elemente de vulnerabilitate pentru infrastructurile critice ale societății.

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

• evenimente naturale şi accidente tehnice ce pot provoca daune materiale, ecologice şi umane importante;

• erori umane şi omisiuni, care prin suportul fizic al societății informatice – societatea cunoaşterii, pot 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 şi risc pentru societățile occidentale avansate, ele vor reprezenta elemente de *input* negativ şi stres pentru societatea românească, ca societate informatică – societate a cunoştințelor. Deci, trebuie depuse de la început eforturi pentru cunoaşterea, localizarea şi minimizarea efectelor potențial negative ce pot apare în societatea informatică – societate a cunoaşterii, infrastructurile critice ale societății.

Privind definirea direcțiilor de construcție şi de coordonare a eforturilor societale pentru societatea informatică – societatea cunoaşterii, se vor evidenția în continuare o serie de aspecte:

- necesitatea schimbului reciproc de informații, date şi cunoştințe referitor la vulnerabilitatea diferitelor sisteme de infrastructuri critice, între Guvern şi sectoarele implicate, transversal între sectoare distincte în cadrul conceptului de infrastructuri critice, în condițiile societății informatice – societatea cunoaşterii;
- necesitatea construirii în cadrul societății informatice – societatea cunoaşterii, a unui sistem de responsabilități care să garanteze cooperarea între diferitele grupuri active în funcționarea infrastructurilor critice;
- protecția infrastructurilor impune construirea de capabilități integrate în cadrul diverselor instituții în structura generală a societății, în România;
- necesitatea realizării unei *culturi de securitate* (safety culture) corespunzătoare;
- sistemul de legi ale societății informatice – societatea cunoaşterii trebuie să ia în considerare potențialul de impact al pericolelor cibernetice şi reglementate în mod corespunzător;
- se impune inițierea şi coordonarea adecvată a unor activități de cercetare ştiințifică care să abordeze problematica vulnerabilității şi securității infrastructurilor critice în cadrul conceptului de societate informatică – societatea cunoaşterii.

Concluzii

Țări precum Australia şi Canada şi-au dezvoltat un proces complex din mai mulți paşi pentru protecția infrastructurii, în conformitate cu propriile lor nevoi. Oricum, cercetările efectuate pentru condiții specifice în analiza infrastructurilor informaționale critice sunt sărace şi majoritatea elementelor metodologice derivă din analiza şi din modelarea riscurilor.

În toate țările au fost implicați cu precădere specialiştii. De aici rezultă că elementele cruciale le dețin specialiştii, care adesea sunt în afara sferei de influență a statului. De asemenea, instituțiile academice au rol minor în comparație cu experții şi consultanții din domeniul protecției infrastructurilor de informații critice.

- În Australia, un proces specific de apărare în mai mulți paşi a fost dezvoltat implicând un număr variat de experți din industrie şi apărare.
- În Canada, un prim efort rezultat în structurarea profilelor infrastructurii, include efectuarea de studii critice privind probabilitatea de apariție a unui eşec. Pe această bază, a fost dezvoltat un proces cuprinzător de protecție a infrastructurii cu atenție deosebită pe identificarea interdependențelor. Matricea dependențelor şi algoritmii sunt folosiți pentru măsurarea şi modelarea efectelor de undă a dependențelor directe.
- În Olanda, doi consultanți au tratat prin segmente infrastructura ICT şi Internetul. Aceste studii dezvoltă un număr de modele prin care clarifică rolul participanților implicați, la fel ca sporirea gradului de înțelegere a interdependențelor.
- În Norvegia, programul guvernamental pentru protecția societății foloseşte un model multicriterial pentru efectuarea analizei de tip cost-eficacitate, pentru studierea vulnerabilităților în sistemele de telecomunicații şi sugerarea costurilor efective ale măsurilor de reducere a acestor vulnerabilități.
- În Elveția, analiza pas cu pas, cu şapte elemente rămâne ipotetic el neavând implementări cantitative. Oricum, schița procesului şi analizei tehnologice a fost realizat pentru diferite sectoare de reprezentanțele InfoSurance.
- În SUA, cercetările privind inderdependențele afacerilor sunt în continuă dezvoltare. Simulările pe calculator sunt dezvoltate de curând, pentru prognoza interacțiunilor dintre elementele critice ale infrastructurii. Pe lângă Departamentul Energiei, care este foarte activ în acest domeniu, un apreciat proces privind vulnerabilitate a fost dezvoltat de CIAO pentru departamentele şi agențiile federale civile.

• Lista de sectoare critice elaborată de SUA, în anul 1977, a creat o puternică impresie în țările dezvoltate.

• Dezvoltarea Internetului duce inerent la insecuritate.

• Activitatea organizațiilor de tip Public-private Partnerships.

• Activitățile interguvernamentale.

• Avertizarea timpurie este percepută ca una dintre realizările marcante de tip CIIP.

• Atacurile din SUA, din septembrie 2001, au avut un puternic impact în CIIP – de atunci multe țări au politici CIIP.

• Legislația veche referitoare la CIIP trebuie atent analizată, mai ales după septembrie 2001.

• Sectoarele critice – în multe țări definiția sectoarelor critice este încă subiect de discuții. Astfel, lista sectoarelor critice nu este încă stabilită.

Sectoarele critice menționate cel mai frecvent în toate țările:

- Sistemul bancar şi financiar.
- Guvernul/serviciile guvernamentale.
- Comunicațiile/tehnologia informatică.
- Urgența/serviciile de salvare.
- Energia/electricitatea.
- Serviciile medicale.
- Transporturile/suport logistic/distribuție.
- Alimentarea cu apă.

Toate țările sunt în stadii foarte diferite în dezvoltarea propriilor structuri de informații critice, iar forța de muncă şi resursele alocate variază foarte mult. Multe țări recunosc necesitatea pentru o cercetare mai amănunțită şi o cuprinzătoare dezvoltare a modelelor şi a metodelor de analiză a diferitelor aspecte ale propriilor CII naționale.

Bibliografie

Dr. Brewer D., *Security Risk Management – the only Reliable Way to tame the information Monster.*

Acad. Drăgănescu M., *Societatea Informațională şi a cunoaşterii. Vectorii Societății Cunoaşterii.*

Gheorghe A., *Analiza de risc şi de vulnerabilități pentru structurile critice ale societății informatice – societate a cunoaşterii.*

Patriciu V.V., Petroşanu M., Bica I., Cristea C., *Securitatea informatică în Unix şi Internet*, Editura Tehnică, 1998.

Wenger A., Metzger J., Dunn M., *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* – Issue 2002

A. Wenger, J.Metzger, M.Dunn, *The International CIIP Handbook: Evolution of the Critical Information Infrastructure Protection (CIIP)* Issue, 2004.

*** *Critical Foundations. Protecting America's Infrastructures*. The Report of the President's Commission on Critical Infrastrucutre Protection, Washington DC, October 1997.

*** *Infosurance*, Zürich, 2001.