SECURITATEA CIBERNETICĂ A INFRASTRUCTURILOR CRITICE ÎNTR-O LUME DIN CE ÎN CE MAI CONECTATĂ

THE CYBER SECURITY OF CRITICAL INFRASTRUCTURES IN A WORLD THAT'S INCREASINGLY CONNECTED

CYBERSÉCURITÉ DES INFRASTRUCTURES CRITIQUES DANS UN MONDE DE PLUS EN PLUS CONNECTÉ

Lt.col.dr.ing. Vasile Florin POPESCU*

Într-o lume din ce în ce mai conectată, infrastructurile critice au devenit mai vulnerabile ca niciodată la amenințările de securitate cibernetică, fie că provin din state naționale, organizații criminale sau persoane fizice. Această nouă vulnerabilitate este cauzată de schimbările fundamentale ale sistemelor tehnologice ale organizațiilor guvernamentale și private. În acest sens, infrastructura critică virtuală a oricărei organizații/națiuni reprezintă o arenă în care securitatea este imperativă. Protecția cibernetică a devenit crucială în fiecare sector de activitate, iar absența unor măsuri pentru protecția infrastructurilor critice amenință să producă daune imense în funcționarea societății.

In an increasingly connected world, critical infrastructures have become more vulnerable than ever to cyber security threats, whether they come from national states, criminal organizations or individuals. This new vulnerability stems from fundamental changes in the technological systems of organizations (government and private). In this regard, the Virtual Critical Infrastructure of any organization / nation represents an arena where security is absolutely imperative. Cyber protection has become crucial in every sector of activity, and the absence of measures to protect critical infrastructures threatens to cause huge damage to the functioning of the company.

Dans un monde de plus en plus connecté, les infrastructures critiques sont devenues plus vulnérables que jamais aux menaces de cybersécurité, qu'elles proviennent d'États nationaux, d'organisations criminelles ou d'individus. Cette nouvelle vulnérabilité est le résultat des changements fondamentaux des systèmes technologiques des organisations (gouvernementales et privées). À cet égard, l'Infrastructure critique virtuelle de toute organisation/nation représente une arène où la sécurité est absolument essentielle. La cybersécurité est devenue indispensable dans tous les secteurs d'activité et l'absence des mesures de protection des infrastructures critiques peut beaucoup nuire au fonctionnement de la société.

Cuvinte-cheie: infrastructuri critice; spațiu cibernetic; amenințări cibernetice; vulnerabilități; sisteme de tehnologie informațională și operațională.

Keywords: *critical infrastructures; cyber space; cyber threats; vulnerabilities, information and operational technology systems.*

Mots-clés: *infrastructures critiques; cyberespace; cybermenaces; vulnérabilités; technologies de l'information et systèmes opérationnels.*

Avioane deturnate de la cursul normal. Garnituri de metrou blocate în tunelele de sub orașe. Baraje sparte care inundă orașe. Pene de electricitate. Telecomunicații blocate. Apeluri de urgență 112 inutilizabile. Aceste momente de haos și panică și alte consecințe potențiale ale atacurilor la adresa infrastructurii critice pot, în cel mai bun caz, să provoace doar astfel de inconveniente, iar în cel mai rău caz, pot duce la pierderi de vieți omenești sau la distrugeri la scară largă.

* ***Ministerul Apărării Naționale***
e-mail: *popescuveve@gmail.com*

Astăzi, aproximativ jumătate din populația lumii trăiește în zone urbane și se presupune că procesul de urbanizare se va accentua, astfel încât doar o treime dintre locuitorii planetei va locui în afara

zonelor urbane până în 2050[1]. Această dezvoltare ridică o serie de provocări care influențează și infrastructurile, a căror funcționare fiabilă și eficientă va determina modul în care orașele sunt capabile să răspundă cerințelor calității vieții[2]. Unele dintre aceste infrastructuri sunt numite „critice”, întrucât bunăstarea societății se bazează fundamental pe fiabilitatea lor. Ele pot fi înțelese ca elemente fundamentale ale sustenabilității societății, siguranței și securității aprovizionării. Infrastructurile critice oferă oamenilor acces la o gamă largă de mărfuri, a căror disponibilitate[3] este esențială pentru rezistența comunităților[4].

Conform Oxford English Dictionary, structura morfematică a termenului *infrastructură* este o combinaţie a prefixului „infra”, cu înţelesul de „sub”, și a rădăcinii cuvântului, purtătoare a semnificației lexicale, anume, „structura”, arată cum este construit un mecanism. Asocierea termenului „critic” celui de „infrastructură” definește acel tip de infrastructură, care, perturbată, poate conduce la pagube majore.

Caracterul critic al infrastructurilor este dat de următoarele:

- unicitatea lor;
- caracterul vital în funcţionarea sistemelor economice, sociale, politice, militare, informaţionale etc.;
- sensibilitatea la schimbări;
- vulnerabilitatea ridicată la ameninţările din mediul extern.

În funcţie de importanţa lor în funcţionalitatea sistemelor și proceselor, infrastructurile se împart în trei categorii[5]:

- infrastructuri obişnuite;
- infrastructuri speciale;
- infrastructuri critice.

Infrastructurile critice sunt împărţite în două categorii importante[6]:

- *fizice*:
  - internaţionale;
  - ale economiei statelor;
  - ale diferitelor sectoare industriale;
  - ale întreprinderilor/companiilor;
  - ale proiectelor;
  - ale transportului aerian, feroviar, naval;
  - ale sistemului financiar;
  - ale locuinţei, localităţii, ţării, continentului;
  - militare;
  - ale sistemului de ordine publică;
  - ale sistemului informaţional şi de siguranţă a statului;
  - ale sistemului sanitar şi de protecţie a cetăţeanului, familiei şi comunităţii
- *virtuale*:
  - ale sistemelor de comunicaţii;
  - ale reţelelor şi bazelor de date;
  - ale spaţiului cibernetic.

Într-o lume din ce în ce mai conectată, infrastructurile critice au devenit mai vulnerabile ca niciodată la amenințările de securitate cibernetică, fie că provin din state naționale, organizații criminale sau persoane fizice. Această nouă vulnerabilitate este cauzată de schimbările fundamentale ale sistemelor tehnologice ale organizațiilor guvernamentale și private. Astfel de organizații – armată, poliție, pompieri, furnizori de servicii medicale și utilități, sisteme bancare, sisteme de transport etc. – acționează cu două tipuri de sisteme tehnologice: sisteme de tehnologie informațională și sisteme de tehnologie operațională.

Sistemele de tehnologie informațională asigură funcțiile de bază ale biroului, cum ar fi comunicarea prin e-mail, salarizare, resurse umane etc., în timp ce sistemele de tehnologie operațională controlează echipamentele fizice și personalul necesar îndeplinirii misiunii lor.

În trecut, sistemele de tehnologie operațională constau din sisteme de sine stătătoare, care le făceau sigure. Acum, sistemele de tehnologie operațională rulează pe aceleași platforme software și hardware cunoscute, ca și sistemele IT. Aceste sisteme sunt bine cunoscute de hackeri și, prin urmare, sunt semnificativ mai puțin sigure.

Ce a dus la această convergență a sistemelor de tehnologie informațională cu sistemele de tehnologie operațională? Iată câteva exemple:

Un proprietar de casă reglează de la distanță termostatul la reședința sa, pentru a scădea temperatura, în timp ce este în vacanță. Un medic vizualizează consumul de insulină al pacienților pe un computer din birou. Companiile monitorizează de la distanță starea și locația trenurilor, autobuzelor și camioanelor, fluxul de petrol și gaze prin conducte, sau consumul de apă ori de energie electrică, pentru a gestiona aceste servicii în mod eficient.

În timp ce tehnologiile din aceste exemple ne îmbunătățesc viața, ele ne pot face în același timp vulnerabili.

Menționez asta, deoarece, pe măsură ce numărul dispozitivelor interconectate continuă să crească, numărul potențialelor puncte de acces pentru hackeri care perturbă infrastructura critică crește și el.

În acest sens, Infrastructura critică virtuală a oricărei organizații/națiuni reprezintă o arenă în care securitatea este imperativă. Protecția cibernetică a devenit crucială în fiecare sector de activitate, iar absența unor măsuri pentru protecția infrastructurilor critice amenință să producă daune imense în funcționarea societății în ansamblu.

Spațiul virtual sau cibernetic reprezintă un set de mijloace și proceduri, bazate pe tehnologia informației și comunicațiilor (TIC) și este format din hardware, software, Internet, servicii de informare și sisteme de control, devenind o infrastructură critică esențială pentru activitatea socioeconomică a oricărei națiuni, organizaţii sau proiect transnațional. Diferite dicționare și enciclopedii definesc spațiul cibernetic astfel:

• Spațiul cibernetic este o rețea de calculatoare formată dintr-o rețea mondială de rețele de calculatoare care folosește protocoale de rețea TCP/IP, pentru a facilita schimbul de date (sursa: Dicționarul Român Online);

• Spațiul cibernetic este mediul electronic de rețele de calculatoare, în care are loc comunicarea online[7].

• O metaforă pentru a descrie terenul nonfizic creat de sistemele informatice: Sistemele online creează un spațiu cibernetic în care oamenii pot comunica unul cu altul, fac cercetări sau, pur și simplu, cumpără[8].

• Spațiul cibernetic este un domeniu caracterizat de utilizarea dispozitivelor electronice și spectrului electromagnetic pentru a stoca, a modifica și a schimba date prin intermediul sistemelor de rețea și infrastructurilor fizice asociate. De fapt, spațiul cibernetic poate fi considerat ca interconectarea dintre ființele umane prin intermediul calculatoarelor și telecomunicațiilor, indiferent de poziţia geografică[9].

Guvernul SUA definește spațiul cibernetic ușor mai larg: Directivele prezidențiale de securitate națională nr. 23 şi 54 definesc spațiul cibernetic ca fiind rețeaua interdependentă a infrastructurilor de tehnologia informației, care include Internetul, rețelele de telecomunicații, sistemele informatice, utilizatorii, precum și cei care controlează industriile critice. Utilizarea comună a termenului se referă, de asemenea, la mediul virtual de informații și la interacțiunile dintre oameni.

Definițiile oferite de Webster, Wikipedia sau Dicționarul Oxford nu sunt absolute și suficient de cuprinzătoare. Conceptul de spațiu virtual s-a extins între timp, incluzând comerțul, finanțele, energia, Bursele de Valori etc.

Obiectivele atacurilor din mediul virtual pot fi clasificate în trei grupe majore:

• sectorul public, agenţiile guvernamentale;

• sectorul privat, în principal, operatorii de infrastructuri critice;

• cetățenii.

Atacurile cibernetice la adresa infrastrucurii critice virtuale pot fi clasificate, în funcție de sursă și de impactul acestora, astfel:

• *Atacurile sponsorizate de state*

Lumea reală şi conflictele fizice s-au extins în lumea virtuală a spațiului cibernetic. În ultimii ani, au fost detectate atacurile cibernetice împotriva infrastructurilor critice ale diferitelor țări și obiectivelor specifice. Câteva exemple cunoscute publicului larg sunt: atacul cibernetic din Estonia, în 2007, care a dus la dezactivarea temporară în mare parte a infrastructurilor critice ale țărilor baltice, atacul cibernetic lansat de Rusia împotriva Georgiei, în 2008, ca un preludiu la invazia terestră, cazul Stuxnet, cu atacuri cibernetice împotriva sistemelor SCADA, cazul Duqu, cu atacuri cibernetice împotriva organizațiilor industriale, atacurile cibernetice suferite de rețelele clasificate ale Guvernului Statelor Unite, comise de către hackeri de pe teritoriul chinez etc.

În ultimii ani, unele state au investit importante resurse economice, tehnice și umane în dezvoltarea amenințărilor avansate persistente (AAP), care atacă agresiv și aleg obiective foarte specifice, în scopul de a menține o prezență constantă în cadrul rețelelor posibilelor victime. Atacurile AAP sunt foarte dificil de detectat, din cauza faptului că utilizează tehnici și componente care sunt special proiectate pentru a se infiltra și rămâne în rețea fără a fi detectate.

• *Atacurile sponsorizate de către organizații private*

Obiectivul multor organizații private este de a obține secrete industriale și economice de la alte organizații competitoare, acest tip de atac fiind de multe ori executat cu sprijin guvernamental.

• *Terorismul, extremismul politic și/sau ideologic*

Terorismul și grupurile extremiste folosesc spațiul cibernetic pentru a planifica și a publica acțiunile lor și pentru a racola adepți care să le efectueze. Aceste grupuri recunosc importanța strategică și tactică a spațiului cibernetic pentru interesele lor, rețelele social media și forumurile devenind principalul instrument utilizat.

• *Atacurile grupurilor de crimă organizată*

Bandele de crimă organizată, cunoscute şi sub numele de bande informatice, au început să își desfășoare activitatea în spațiul cibernetic, exploatând posibilitatea anonimatului pe care acest domeniu o oferă. Obiectivul acestor tipuri de bande este de a obține informații sensibile pentru utilizarea, ulterioară, a acestora frauduloasă și pentru câștiguri economice semnificative.

• *Hackerii*

Odată cu apariţia Internetului, dar mai ales în ultimii ani, activităţile hackerilor au devenit una dintre cele mai mari ameninţări la adresa guvernelor și organizațiilor de orice natură. Principiile acestei agresiuni sunt anonimatul și distribuirea gratuită de informații în spațiul cibernetic, în esență, prin intermediul Internetului. Misiunea lor este de a „ataca” spațiul cibernetic, reprezentat de persoane sau de organizațiile care încalcă oricare dintre principiile sau intereselor lor. Acest lucru implică faptul că spațiul cibernetic al guvernelor din majoritatea țărilor din întreaga lume, al băncilor, al companiilor de telecomunicații, al furnizorilor de infrastructură critică, al furnizorilor de servicii de Internet, în ansamblu, tot spațiul cibernetic, sunt susceptibile de a fi hackuite cu obiectivul principal de a fura informații sensibile.

• *Atacurile personalului cu acces privilegiat (cei din interior)*

Aceste grupuri reprezintă una dintre cele mai mari ameninţări la adresa securității spațiului cibernetic al națiunilor, deoarece ele sunt, de cele mai multe ori, parte integrantă a tuturor atacurilor menționate anterior, putând fi emise de un spion sau de un angajat care lucrează pentru bande de teroriști sau infractori cibernetici, de angajați nemulțumiți etc.

Concluzii

Necesitatea de a stimula apărarea cibernetică pentru infrastructurile critice este clară. Dar întrebarea devine acum: Cum ajungem acolo? În acest sens, am dezvoltat câteva recomandări pentru a contribui la acțiuni colective eficiente.

• Elaborarea unei strategii naționale de educație cibernetică: pentru a proteja cu adevărat infrastructura critică, trebuie să avem persoane calificate. Prin urmare, este necesar ca educația cibernetică să devină o prioritate în procesul educațional. România nu are o strategie de educație în domeniul cibersecurității care să alimenteze și să finanțeze centre naționale de excelență în domeniu.

• O altă recomandare este mentoratul transorganizațional și transferul de cunoștințe. Organizațiile cu mai puțină experiență de securitate cibernetică sau echipele mai mici de cibersecuritate pot învăța de la colegii lor mai experimentați. Organizațiile mai mari ar trebui, de asemenea, să-și încurajeze experții să participe la asociații din industrie, în cadrul unor parteneriate public-private și organizații regionale, care să ofere toate oportunitățile de formalizare a îndrumării interorganizaționale și ale transferului de cunoștințe.

• Crearea unor strategii mai bune de partajare a informațiilor între sectorul guvernamental/de stat și sectorul privat: experții în securitate cibernetică par, în mare măsură, să fie de acord cu faptul că, pentru un nivel optim de securitate în toate sectoarele, cooperarea este esențială.

• Efectuarea de exerciții de scenarii pentru potențiale crize: când vine vorba despre infrastructură critică, un dezastru real nu este cadrul propice care să ne determine să învățăm din greșeli. O astfel de pregătire trebuie să aibă loc în avans, în exerciții de scenarii la crize care să simuleze modul în care o echipă de răspuns ar face față unui incident neașteptat.

NOTE:

1 M. Rizea et al., UN (United Nations), *World Urbanization Prospects: The 2018 Revision, Key Facts*, 2018, https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf, accesat la 10 noiembrie 2018.

2 S. Riffat, R. Powell, D. Aydin, *Future cities and environmental sustainability. Future Cities Environ*, 2016.

3 A.H. Hay, S. Willibald, *Making Resilience Accessible. Access: An Enabler of Community Resilience*, Southern Harbour, 2017, https://www.southernharbour.net/assets/docs/SH_Access%20WhitePaper_2017_0307%C6%92.pdf, accesat la 14 ianuarie 2019.

4 A. Hay, *Surviving catastrophic events: Stimulating community resilience. In Infrastructure Risk and Resilience*, Transportation, IET, Stevenage, UK, 2013, pp. 41-46.

5 G. Alexandrescu, Gh. Văduva, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.

6 G. Alexandrescu, Gh. Văduva, *op.cit.*

7 http://en.wikipedia.org/wiki/Cyberspace

8 http://www.webopedia.com/TERM/C/cyberspace.html

9 http://searchsoa.techtarget.com/definition/cyberspace

BIBLIOGRAFIE

Alexandrescu G., Văduva Gh., *Infrastructuri critice. Pericole, ameninţări la adresa acestora. sisteme de protecţie*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2006.

Hay A., *Surviving catastrophic events: Stimulating community resilience. In Infrastructure Risk and Resilience*, Transportation, IET, Stevenage, UK, 2013.

Hay A.H., Willibald S., *Making Resilience Accessible. Access: An Enabler of Community Resilience*, Southern Harbour. 2017, https://www.southernharbour.net/assets/docs/SH_Access%20WhitePaper_2017_0307%C6%92.pdf

Riffat S., Powell R., Aydin D., *Future cities and environmental sustainability. Future Cities Environ*, 2016.

Rizea M. et al., *UN (United Nations). World Urbanization Prospects: The 2018 Revision*, Key Facts. 2018, https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf

http://en.wikipedia.org/wiki/Cyberspace

http://searchsoa.techtarget.com/definition/cyberspace

http://www.webopedia.com/TERM/C/cyberspace.html