RISCURI ŞI AMENINŢĂRI CIBERNETICE LA ADRESA SECURITĂŢII INTERNAŢIONALE. TERORISMUL CIBERNETIC - UN FLAGEL CARE AMENINŢĂ SECURITATEA GLOBALĂ

CYBER RISKS AND THREATS TO INTERNATIONAL SECURITY. CYBER TERRORISM – A SCOURGE THREATENING GLOBAL SECURITY

Gl. mr. (r) prof. univ. dr. Visarion NEAGOE*
Drd. Mr. Silviu-Stelian BORŞA**

Rezumat: *În zilele noastre, totul este controlat de tehnologie şi mai ales de computere. Ameninţările cibernetice la adresa unui sistem controlat se referă la persoanele care încearcă să obţină acces neautorizat la un dispozitiv şi/sau o reţea, folosind o cale de comunicaţie a datelor. Acest acces poate fi direcţionat din interiorul unei organizaţii, de către utilizatori din cadrul organizaţiei respective, sau din locaţii externe, de persoane necunoscute care folosesc internetul. Ameninţări la adresa sistemelor de control pot veni din numeroase surse, printre care guverne ostile, grupări teroriste, angajaţi nemulţumiţi, şi intruşi răuvoitori. Ameninţarea potenţială pe care o reprezintă terorismul cibernetic a declanşat un semnal de alarmă deosebit de serios. Numeroşi specialişti în securitate, politicieni şi alţii au vorbit despre pericolele asociate teroriştilor cibernetici care ar pătrunde în sistemele de computere guvernamentale şi private, producând daune considerabile în domeniile militar, financiar, de servicii ale statelor cu economie avansată. Fără îndoială, terorismul cibernetic este o opţiune foarte avantajoasă pentru teroriştii zilelor noastre, care pun mare preţ pe posibilitatea oferită de acesta de a rămâne în anonimat şi de a provoca pagube considerabile, ca şi pe impactul său psihologic şi atractivitatea pentru media. Pentru a contracara aceste ameninţări este necesară crearea unei bariere cibernetice sigure care să protejeze sistemul; astfel, statele se confruntă cu provocarea de a crea o societate „invulnerabilă" din punct de vedere cibernetic, dar în care să funcţioneze în continuare drepturile şi libertăţile democratice actuale. De asemenea, trebuie găsite soluţii pentru această problemă complicată, fără a întrerupe conexiunile curente şi sistemele aflate în funcţiune în momentul de faţă, astfel încât efectul resimţit de societate să fie menţinut la un nivel acceptabil.*

* Membru corespondent al Academiei Oamenilor de Ştiinţă din Romania, E-mail: visarionneagoe@yahoo.com
** Doctorand la Universitatea Naţională de Apărare „Carol I", E-mail: borsaliviu1979@gmail.com
[1] *Strategia cibernetică de securitate a României*, 2013, p.4.

Cuvinte-cheie: *terrorism cibernetic; extorcare cibernetică; mediu virtual; spaţiu cibernetic; hacker; strategie cibernetică; ameninţare cibernetică; imposibilitate de accesare; reţea; organizaţie teroristă.*

Abstract:. *Nowadays technology and particularly computers are controlling everything. Cyber threats against a controlled system refer to persons who attempt unauthorized access to a device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. The potential threat posed by cyber terrorism has raised considerable alarm. Numerous security experts, politicians, and others have publicized the danger associated with cyber terrorists hacking into government and private computer systems and crippling the military, financial, and service sectors of advanced economies. Cyber terrorism is, to be sure, an attractive option for modern terrorists, who value its anonymity, its potential to inflict massive damage, its psychological impact, and its media appeal. To protect against these threats, it is necessary to create a secure cyber-barrier around; the states are facing the challenge of creating a "cyber proof" society while maintaining the actual democratic liberties. Also, they have to seek solutions to this complicated issue, without interrupting the current connections and systems in place, so the effect on society is kept to an acceptable level.*

Keywords: *cyber terrorism; cyber extortion; virtual environment; cyber space; hacker; cyber strategy; cyber threat; denial-of-service; network; terrorist organization.*