Ioana VASIU **Lucian VASIU**

CRIMINALITATEA ÎN CYBERSPAȚIU

Universul Juridic
București
-2011-

Editat de **S.C. Universul Juridic S.R.L.**

Descrierea CIP a Bibliotecii Naționale a României
VASIU, IOANA
Criminalitatea în cyberspațiu / Ioana Vasiu, Lucian Vasiu. - București : Universul Juridic, 2011
ISBN 978-973-127-674-8

I. Vasiu, Lucian

004.056.5
343.23:004

REDACȚIE: tel./fax: **021.314.93.13**
tel.: **0731.121.218**
e-mail: **redactie@universuljuridic.ro**

DEPARTAMENTUL DISTRIBUȚIE: telefon: **021.314.93.15; 0726.990.184**
tel./fax: **021.314.93.16**
e-mail: **distributie@universuljuridic.ro**

CUVÂNT ÎNAINTE

Studiul criminalității informatice s-a îmbogățit cu o nouă lucrare remarcabilă a reputaților specialişti în materie **Ioana Vasiu** *şi* **Lucian Vasiu.**

Deşi cei doi cunoscuți specialişti nu sunt la prima lucrare în acest domeniu, de astă dată s-au întrecut pe ei înşişi elaborând un adevărat tratat de drept penal special informatic, analizând nu numai problemele generale pe care le ridică criminalitatea informatică (sistemele informatice, prevenirea criminalității informatice, amenințări la adresa sistemelor informatice), dar şi infracțiunile care se comit în acest domeniu (infracțiuni în cyberspațiu, definiție, clasificări, categoriile de infracțiuni informatice).

Deosebit de important este şi ultimul capitol (partea a III-a), consacrat mijloacelor procedurale şi tehnice de prevenire a criminalității în cyberspațiu (politici şi proceduri), analiza de risc, atenuarea riscurilor, controale tehnice.

Lucrarea este deosebit de interesantă prin ampla documentare de specialitate pe care o are la bază, cât şi prin multiplele probleme noi pe care le abordează în legătură cu criminalitatea informatică.

Autorii analizează pe larg dezbaterile şi controversele care au loc în acest nou domeniu al cunoaşterii ştiințifice şi al tehnicii informatice, exprimând păreri personale competente asupra evoluției şi perspectivelor pe care le oferă cunoaşterea şi prevenirea criminalității informatice.

Valoroase sunt şi trimiterile la legislația penală europeană, cît şi a unor state nord-americane, precum şi informațiile asupra programelor unor societăți internaționale în materie de criminalitate informatică.

Se citesc cu mare interes, de asemenea, exemplificările cu care autorii îşi întregesc demonstrațiile şi expunerile privitoare la ultimele congrese ale Națiunilor Unite privind problemele de prevenire a criminalității.

Lucrarea este rodul unor eforturi creatoare notabile ale autorilor, care s-au străduit şi au reuşit să pună la dispoziția cititorului român interesat de problematica criminalității informatice o carte valoroasă, plină de informații şi reflecții asupra unui fenomen care preocupă întreaga comunitate internațională.

Prof. univ. dr. George Antoniu
Bucureşti, 20 octombrie 2011

INTRODUCERE

Încă din cele mai vechi timpuri, rețelele au oferit oportunități pentru dezvoltare şi inovație şi au furnizat o structură pentru sistemele economice şi sociale. De la drumurile şi apeductele romane până la sistemul de drumuri din secolul al XIX-lea şi la rețelele de sateliți şi telecomunicații din zilele noastre, capacitățile oferite de rețele au fost folosite pentru a depăşi barierele de timp şi spațiu şi pentru a deschide noi frontiere pentru interacțiunea şi activitățile umane[1]. Răspândirea largă a calculatoarelor nu este chestiune de „modă" sau hiperbolă, cu toate că există multe asemenea elemente în literatura de specialitate – este un proces ireversibil, cu implicații majore asupra vieții şi activității umane[2], care, în mai puțin de o generație, a schimbat semnificativ societatea actuală.

Revoluția informatică a fost comparată cu revoluția industrială referitor la impactul asupra societății[3]: cu excepția electrificării, nicio altă invenție tehnologică nu a afectat atât de fundamental modul în care oamenii trăiesc, lucrează, învață, comunică sau fac afaceri. Aplicațiile tehnologiilor informației şi comunicațiilor în zilele noastre sunt

---

[1] Vezi R. J. Gordon, *Does the „New Economy" Measure up to the Great Inventions of the Past?*, NBER Working Paper No. w7833 (2000); J. S. Landefeld şi B. M. Fraumeni, *Measuring the New Economy*, Bureau of Economic Analysis (2000); President's Information Technology Advisory Committee, *Information Technology Research: Investing in Our Future*, Report to the President (1999); E. Brynjolfsson şi S. Yang, *The Intangible Costs and Benefits of Computer Investments: Evidence from the Financial Markets* (1999).

[2] Vezi H. C. Jr. Lucas, *Information technology and physical space*, COMMUNICATIONS OF THE ACM, November, 44 (11), 89-96 (2001); OECD, *The new economy beyond the hype* (2001).

[3] Vezi, spre exemplu, D. S. Alberts şi D. S. Papp (eds.), *The Information Age: An Anthology on Its Impact and Consequences* (1997); M. Castells, *The Rise of the Network Society* (1996); C. Freeman, L. Soete şi U. Efendioglu, *Diffusion and the Employment Effects of Information and Communication Technology*, INTERNATIONAL LABOR REVIEW, 134, 4-5, 587-603 (1995).

extrem de diverse, practic în toate domeniile calculatorul este, dacă nu absolut necesar, cel puțin foarte util. Printre domeniile în care calculatorul este utilizat pe scară largă amintim: juridic[1], guvernamental[2], creației vestimentare[3], financiar-bancar[4], industrial, educației, militar, artistic, jurnalistic, cinematografic, televiziune, medical etc.[5]

Rețelele de comunicații electronice, în mod deosebit Internetul[6], permit o inovație crescută[7], obținerea de avantaje competiționale[8], stocarea, procesarea şi transmiterea de cantități imense de date şi crearea de noi piețe[9], reducerea numărului de erori potențiale cauzate

---

[1] Vezi S. Pallaras, *New technology: opportunities and challenges for prosecutors*, CRIME, LAW AND SOCIAL CHANGE, Aug, 71-89 (2011); I. Vasiu şi L. Vasiu, *Informatică juridică şi Drept informatic 2009*, Ed. Albastră, Cluj-Napoca (2009); O. Rabinovich-Einy, *Beyond efficiency: The transformation of courts through technology*, UCLA JOURNAL OF LAW & TECHNOLOGY, Vol. 12, Iss. 1, Spring (2008).

[2] Vezi, spre exemplu, I. Vasiu şi L. Vasiu, *Top Management Skills in E-Government: A Conceptual Framework*, JOURNAL OF E-GOVERNMENT, 2 (3), 5-17 (2006).

[3] Vezi *Intellectual property in the fashion industry*, WIPO MAGAZINE, May-June (2005).

[4] Vezi B. F. Kubiak şi M. F. Kowalik, *Marketing Information Systems As A Driver Of An Organization's Competitive Advantage*, JOURNAL OF INTERNET BANKING AND COMMERCE, vol. 15, No. 3, December (2010); L. R. Klein, C. Saltzman şi V. G. Duggal, *Information Technology and Productivity: The Case of the Financial Sector* (2003).

[5] Vezi D. W. Jorgenson, *Information Technology and the G7 Economies*, în *Hard-to-Measure Goods and Services: Essays in Honor of Zvi Griliches* (E. R. Berndt şi C. R. Hulten, ed.) (2007).

[6] Vezi J. L. Zittrain, *The Generative Internet*, 119 HARVARD LAW REVIEW, 1974 (2006).

[7] Vezi E. Brynjolfsson (interviu), *The four ways IT is revolutionizing innovation*, MIT SLOAN MANAGEMENT REVIEW, vol. 51, No. 3, Spring (2010). Vezi şi OECD, *Information Technology Outlook* (2010).

[8] Vezi, spre exemplu, B. F. Kubiak şi M. F. Kowalik, *Marketing Information Systems as a Driver of an Organization's Competitive Advantage*, JOURNAL OF INTERNET BANKING AND COMMERCE, vol. 15, No.3, December (2010); A. McAfee şi E. Brynjolfsson, *Investing in the IT That Makes a Competitive Difference*, HARVARD BUSINESS REVIEW, July (2008); D. W. Jorgenson, *Information Technology and the G7 Economies*, în *Hard-to-Measure Goods and Services: Essays in Honor of Zvi Griliches* (E. R. Berndt şi C. R. Hulten, ed.) (2007); D.W. Jorgenson şi K. Motohashi, *Information Technology and the Japanese Economy*, NBER Working Paper No. 11801 (2005).

[9] Vezi, spre exemplu, J. D. Levin, *The Economics of Internet Markets*, NBER Working Paper No. 16852 (2011); J. Cha, *Exploring the internet as a unique shopping channel to sell both real and virtual items: A comparison of factors affecting purchase*

de procesări manuale, o mai bună gestionare a stocurilor, o utilizare intuitivă, ceea ce reduce cheltuielile şi timpul alocat pentru pregătirea utilizatorilor, adaptarea unor funcţii conform nevoilor utilizatorilor, posibilitatea de a colabora, cerceta (*virtual research communities*[1]) şi învăța de la distanță[2], de a integra sisteme şi aplicaţii diverse şi posibilitatea efectuării de tranzacţii financiare şi comerciale electronice sau mobile (*e-banking*[3], *m-banking*[4], *m-payment*[5]) prin folosirea de mesaje text (SMS) sau tehnologii precum *Wireless Application Protocol* (WAP), *Universal Subscriber Identity Module*[6] (USIM) sau *Near Field Communication* (NFC).

Ubicuitatea tehnologiilor informaţiei şi comunicaţiilor este reflectată şi de veniturile marilor firme din domeniu: HP peste 126 miliarde; AT&T peste 124 miliarde; IBM circa 100 miliarde; Microsoft circa 62,5 miliarde; Intel 43,6 miliarde; Cisco peste 40

---

intention and consumer characteristics, JOURNAL OF ELECTRONIC COMMERCE RESEARCH, vol. 12, No. 2 (2011); Information Technology Industry Council, *The IT Industry's Cybersecurity Principles for Industry and Government* (2011), care estimează beneficiile globale anuale ale folosirii comerciale a Internetului la circa 1,5 trilioane dolari. Vezi şi A. Barua, P. Konana, A. B. Whinston şi F. Yin, *An Empirical Investigation of Net-Enabled Business Value*, MIS QUARTERLY, 28, 4, 585-620 (2004); T. Dewett şi G. R. Jones, *The Role Of Information Technology In The Organization: A Review, Model, and Assessment,* JOURNAL OF MANAGEMENT, 27, 3 (2001), p. 313 şi urm.; M. E. Porter, *Strategy and the Internet*, HARVARD BUSINESS REVIEW, March (2001).

[1] Vezi G. Andronico, V. Ardizzone, R. Barbera, B. Becker, R. Bruno, A. Calanducci, D. Carvalho, L. Neumann Ciuffo, M. Fargetta, E. Giorgio, G. La Rocca şi A. Masoni, *e-Infrastructures for e-Science: A Global View*, JOURNAL OF GRID COMPUTING, Vol. 9, No. 2, 155-184 (2011).

[2] Vezi, spre exemplu, C. Reimsbach-Kounatze, *Virtual Worlds: Immersive Online Platforms for Collaboration, Creativity and Learning*, OECD Digital Economy Papers, No. 184 (2011).

[3] Vezi J-H. Wu, T.-Li Hsia şi M. S. H. Heng, *Core capabilities for exploiting electronic banking*, JOURNAL OF ELECTRONIC COMMERCE RESEARCH, Vol. 7, No. 2 (2006).

[4] Vezi, spre exemplu, folosirea telefonului mobil pentru a depozita cecuri (*mobile remote deposit capture*): fotografiere faţă şi verso a cecului şi transmiterea imaginilor către instituţia financiară.

[5] Vezi în T. R. McTaggart şi D. W. Freese, *Regulation of Mobile Payments*, THE BANKING LAW JOURNAL, Vol. 127, No. 6, June (2010).

[6] Aplicaţie care rulează pe un card cu cip (*Universal Integrated Circuit Card*) introdus într-un telefon mobil WCDMA 3G.

miliarde (vezi şi *Vision: The Network is the Platform to Change the Way the World Works, Lives, Plays, and Learns* - conform *Annual Report*); Amazon.com, peste 34,2 miliarde; Google 29,3 miliarde; Apple peste 22,3 miliarde[1]. Piaţa mondială a tehnologiilor informaţiei şi comunicaţiilor a atins 2000 miliarde de euro şi creşte în prezent cu o rată de 4% în fiecare an (piaţa europeană reprezintă 34% din această valoare; acest sector reprezintă 4,5% din PIB-ul european)[2]. Investiţiile în cercetare şi dezvoltare în domeniul tehnologiilor informaţiei şi comunicaţiilor sunt, de asemenea, foarte importante în anul 2010, în creştere, de regulă faţă de 2009: Microsoft 8,7 miliarde; Intel 6,6 miliarde (5,7 miliarde în 2009); IBM peste 6 miliarde (peste 5,8 miliarde în 2009); Google 3,762 miliarde (2,843 miliarde în 2009); HP 3 miliarde (faţă de 2,8 miliarde 2009); Apple 1,8 miliarde (în creştere cu 34% faţă de anul precedent); Cisco peste 5,2 miliarde (în creştere cu 1,2% faţă de anul precedent)[3].

Printre cele mai semnificative caracteristici ale societăţii contemporane se numără: Viteza, Voracitatea informaţională şi Vulnerabilitatea.

Viteza

După cum consideră Adam[4], modul de viaţă occidental este asociat cu o abordare particulară a *timpului* şi a *vitezei*: timpul este perceput ca o resursă valoroasă, iar viteza este asociată cu *eficienţa*. Ecuaţia „timpul este bani" este prezentă în toate activităţile şi relaţiile contemporane şi un întreg şir de consecinţe se naşte din decontextualizarea şi relaţia care se formează între timp ca „bani"; atunci când timpul este bani, două consecinţe prezintă un interes particular: cu cât ceva se mişcă mai repede prin sistem, cu atât mai bine este pentru eficienţa şi productivitatea respectivului sistem, respectiv timpul

[1] Conform Raportului anual al firmelor respective, sumele fiind exprimate în dolari.

[2] Vezi Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul regiunilor, COM (2009) 116 final, Bruxelles, 13.3.2009.

[3] Conform Raportului anual al firmelor respective, sumele exprimate în dolari.

[4] Vezi B. Adam, *When Time is Money: Contested Rationalities of Time and Challenges to the Theory and Practice of Work*, Working Paper Series, Cardiff University (2001).

nefolosit este o risipă de bani, de aici dezvoltarea societății care funcționează non-stop – cu siguranță, tehnologiile informației şi comunicațiilor susțin şi impulsionează o asemenea abordare. Dezvoltarea tehnologiilor informației şi comunicațiilor a fost influențată de realizările remarcabile din domeniul electronicii, de la valve termionice şi tranzistori până la circuitele puternic integrate, care au generat un progres tehnologic remarcabil.

Din anii '60 ai secolului trecut, numărul de tranzistori pe microprocesor s-a dublat la fiecare 18-24 luni, rezultând o creştere deosebită a capacității de procesare a calculatoarelor (această dublare este aproximativ echivalentă cu mărirea de 10 ori la fiecare 5 ani şi de 100 de ori la fiecare 10 ani, fenomen cunoscut sub denumirea de *Legea lui Moore*[1]), unele inițiative vizând dezvoltarea de calculatoare *exaflop* (10^{18} operații *floating point* pe secundă) până în anul 2020[2]. La fel de remarcabile au fost avansurile în ceea ce priveşte tehnologiile de stocare (discuri care pot stoca teraocteți, memorii flash de mare capacitate etc.) sau realizarea ecranelor (spre exemplu, *Capacitive touchscreen*, *Haptic technology*, *Retina Display* etc.).

Voracitatea informațională

Informația este o componentă centrală, constitutivă a vieții umane, inerentă relațiilor interpersonale, economice sau de altă natură. Informația, produsele informației, precum şi costurile şi beneficiile rezultate din informație joacă un rol din ce în ce mai mare în societatea contemporană. Adoptarea pe scară largă a tehnologiilor informației şi comunicației a dus la o nouă formă de capitalism, numită *hipercapitalism*[3] sau *capitalism informațional*[4], care depinde esențial de informație şi de sistemele informatice.

---

[1] Fenomen prezis de Gordon Moore, co-fondator al corporației Intel, în anul 1965 – vezi K. Grifantini, *Moore's Law*, TECHNOLOGY REVIEW, Jan/Feb (2009), p. 30; W. R. Bottoms, *Beyond Moore's Law*, CIRCUITS ASSEMBLY, Apr (2008), p. 44; U.S. Department of Commerce, *Digital Economy 2000* (2000). Vezi şi J. G. Koomey, *Outperforming Moore's Law*, IEEE SPECTRUM, vol. 47, Iss. 3 (2010), p. 68.

[2] Vezi *IBM Project Proposes Using Light to Make Chips Faster*, COMPUTER, Feb, 14-15 (2011).

[3] Vezi P. Graham, *Hypercapitalism: Political economy, electric identity, and authorial alienation*, EXPLORING CYBERSOCIETY CONFERENCE (1999).

[4] Vezi T. Morris-Suzuki, *Capitalism in the Computer Age*, în J. Davis, T. Hirschl şi M. Stack (Eds.), *Cutting Edge: Technology, Information, Capitalism and Social Revolution* (1997).

La nivel individual, consumul informației este din ce în ce mai mare. Astfel, în anul 2008, americanii au consumat informație de circa 1,3 trilioane ore (în medie circa 12 ore pe zi), un total de 3,6 *zettaocteți* (un milion de milioane gigaocteți) şi peste 10 trilioane cuvinte (peste 100.000 cuvinte în medie pe persoană)[1]. YouTube serveşte peste 2 miliarde înregistrări video pe zi, circa 10% fiind vizionate pe telefonul mobil (conform Google, *Annual Report 2010*); Facebook are peste 900 milioane obiecte cu care indivizii interacționează (pagini, grupuri, evenimente), peste 2 miliarde de postări sunt 'Like' şi comentate zilnic, peste 250 milioane fotografii sunt încărcate pe zi; peste 7 milioane aplicații şi site-uri web sunt integrate[2]. Traficul IP global anual se estimează că va ajunge la circa 1 zettaoctet până la sfârşitul anului 2015, numărul de dispozitive conectate la rețele IP va fi dublu față de populația globală în 2015, iar traficul IP *per capita* va atinge 11 gigaocteți în 2015 (față de 3 gigaocteți *per capita* în anul 2010)[3].

Vulnerabilitatea

Sofisticata lume a sistemelor informatice este deosebit de ispititoare: o lume digitală unde sunt posibile afaceri de la distanță, documentare eficientă, comunicații instantanee ş.a.; cu toate acestea, lumea tehnologiilor informației şi comunicațiilor nu este deloc lipsită de vulnerabilități, unele dintre acestea asociate cu *criminalitatea în cyberspațiu*[4]. Dezvoltările tehnologiilor informației şi comunicației au

[1] Vezi în R. E. Bohn şi J. E. Short, *How Much Information? 2009 Report on American Consumers* (2010); vezi şi IDG, *The Expanding Digital Universe* (2007).

[2] Vezi statistici Facebook.com (2011).

[3] Vezi Cisco, *Visual Networking Index: Forecast and Methodology, 2010–2015* (2010).

[4] Dovedind o preocupare deosebită pentru prevenirea criminalității informatice, Consiliul Europei a adoptat în 2001 *Convention on Cybercrime*, iar în anul 2002 a lansat *Proposal for a Council Framework Decision on attacks against information systems* (COM(2002) 173 final – Official Journal C 203 E of 27.08.2002. De asemenea, la nivel european a fost creată *European Network and Information Security Agency* (ENISA), prin Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004). Vezi şi Decizia-Cadru 2005/222/JAI a Consiliului din 24 februarie 2005 privind atacurile împotriva sistemelor informatice şi *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems* - COM(2008) 448. Vezi şi U. S. Government Accountability Office, *Cybercrime: Impact and Responses to Cyber Threats* (2008).

dus la un tip de criminalitate ce nu a fost posibilă anterior (spre exemplu, diseminarea contaminanților informatici[1]); pe de altă parte, oferă oportunități crescute de comitere a unor infracțiuni tradiționale (spre exemplu, falsul)[2]. Tendințe recente, cum ar fi *cloud computing* (soluții informatice distribuite deținute de o terță parte, în care utilizatorii nu au posesia fizică a datelor lor), mobilitatea (folosirea de calculatoare portabile sau telefoane mobile[3] inteligente), adoptarea de programe de tip *open source* (care, cel puțin teoretic, prezintă o vulnerabilitate sporită), convergența serviciilor şi rețelelor[4], folosirea *Web 2.0* (site-uri de socializare, blog-uri sau wiki-uri) şi numărul mare de erori potențiale (spre exemplu, erori de design, instalare sau întreținere a programelor informatice[5]) cresc semnificativ vectorii potențiali pentru atacuri informatice. Adițional, numărul foarte mare de utilizatori[6] şi calculatoare pe Internet (*hosts*)[7], posibilitatea de a

[1] Google a anunțat că a descoperit peste 11000 domenii pe Internet implicate în distribuirea de contaminanți informatici (*malware distribution*) – vezi în F. Paget, *Running Scared: Fake Security Software Rakes in Money Around the World* (2010); vezi şi numărul de peste 3400 de site-uri web malițioase blocate zilnic, conform Symantec, *State of Security Survey* (2011).

[2] A se vedea S. W. Brenner, *Cybercrime: criminal threats from cyberspace*, Praeger (2010); S. Fafinski, W. H. Dutton şi H. Margetts, *Mapping and Measuring Cybercrime* (2010); F. Calderoni, *The European legal framework on cybercrime: striving for an effective implementation*, CRIME, LAW AND SOCIAL CHANGE, 339–357 (2010); J. R. E. Bell, *The prosecution of computer crime*, JOURNAL OF FINANCIAL CRIME, 9 (4), 308-325 (2002).

[3] Conform International Telecommunication Union, *The world in 2010*, numărul global al abonamentelor la telefonia mobilă este de circa 5,3 miliarde, incluzând 940 milioane abonamente la servicii 3G.

[4] Vezi Rajendra Singh and Siddhartha Raja, *Convergence in information and communication technology: Strategic and regulatory considerations* (2010).

[5] Vezi B. Schneier, *The Problem Is Information Insecurity*, SECURITY WATCH, August 10 (2008); Web Application Security Consortium, *Web Application Security Statistics Project* (2008).

[6] Conform Internet World Stats, în 31 martie 2011 erau 2,095 miliarde utilizatori (44% în Asia, 22,7% în Europa, 13% în America de Nord); potrivit International Telecommunication Union, *The world in 2010*, numărul utilizatorilor Internet a depăşit 2 miliarde; conform International Bank for Reconstruction and Development/The World Bank, *The Little Data Book on Information and Communication Technology* (2011), există peste 1,8 miliarde utilizatori Internet.

[7] În iulie 2011 erau 849869781 *hosts* pe Internet (818374269 în ianuarie 2011), conform Internet Systems Consortium (2011).

acționa de la distanță, comercializarea atacurilor informatice (oferirea ca produs comercial de contaminanți informatici, acces la *botnet*[1]-uri sau informații pentru realizarea atacurilor[2]) și asimetriile informaționale și, adesea, motivaționale măresc considerabil riscul atacurilor informatice și efectele lor potențiale.

Atacurile informatice pot viza beneficii financiare, intimidare, supraveghere sau manipulare a informațiilor. După cum remarcă în mod corect Comisia Europeană[3], atacurile pe scară largă împotriva sistemelor informatice au devenit din ce în ce mai frecvente, prezintă o dimensiune transfrontalieră considerabilă[4] și au dus la amenințări noi, sofisticate din punct de vedere tehnologic și la o tendință de utilizare a tehnologiilor informației și comunicațiilor în scopul supremației politice, economice și militare, inclusiv prin capacități ofensive. Amenințările pot viza:

- *Exploatare* (cazul *amenințărilor persistente avansate*[5] sau exfiltrarea de informații în scopul spionajului economic sau politic[6], încălcarea drepturilor de proprietate intelectuală etc.);

---

[1] Un număr de calculatoare controlate de un calculator central (*command-and-control*) pentru executarea de comenzi.

[2] Vezi, spre exemplu, R. Anderson, R. Bohme, R. Clayton și Tyler Moore, *Security Economics and European Policy* (2008).

[3] Vezi Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul regiunilor privind protecția infrastructurilor critice de informație, COM(2011) 163 final, Bruxelles, 31.3.2011.

[4] Vezi și UNODC, *Draft collection of topics for consideration within a comprehensive study on impact and response to cybercrime*, 17-21 January (2011).

[5] Acestea sunt definite în US National Institute for Standards and Technology (NIST), *Managing Information Security Risk: Organization, Mission, and Information System View* (2011) ca fiind un adversar care posedă un nivel de expertiză sofisticată și resurse importante care îi pot permite crearea de oportunități pentru realizarea obiectivelor prin utilizarea de vectori de atac multipli.

[6] Vezi, spre exemplu, cazurile GhostNet și Shadow Network: investigarea primului caz a relevat infectarea a 1295 de calculatoare în 103 țări, circa 30% dintre acestea fiind considerate „high value" deoarece aparțineau unor instituții guvernamentale (ambasade, ministere, comisii). Investigarea digitală a evidențiat comunicații între calculatoarele infectate și adrese IP ale unor servere situate în China care au relevat extracția de documente senzitive – vezi ENISA, *Botnets: Detection, Measurement, Disinfection & Defence* (2011).

- S*abotaj* (spre exemplu, atacurile de tip blocarea distribuită a serviciului (*Distributed Denial of Service*) sau spam-urile generate prin botnet-uri (spre exemplu, rețeaua Conficker de 7 milioane de calculatoare sau *spam botnet*-ul Rustock, care putea trimite 30 miliarde de mesaje de poştă electronică pe zi[1]) şi întreruperea mijloacelor de comunicare;
- *Distrugere* fizică[2].

Atacurile informatice ridică probleme noi şi multiple şi pot afecta toate nivelele societății. Atacurile informatice vizează şi afectează persoane fizice din toate grupurile demografice (bărbații şi femeile raportând crime într-o proporție aproape egală[3]), firme mici şi mijlocii (IMM-uri[4]), instanțe de judecată[5], operatori bursieri[6], corporații globale[7], organisme guvernamentale, întregi industrii[8] sau chiar țări

[1] Vezi Microsoft, *Battling the Rustock Threat* (2011).

[2] Vezi cazul Stuxnet, care a distrus fizic o țintă militară, descris în R. Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE SECURITY & PRIVACY, May/June, 49–51 (2011); vezi şi Cisco, *2010 Annual Security Report* (2011).

[3] Vezi Internet Crime Complaint Center, *2010 Internet Crime Report* (2011).

[4] Vezi, spre exemplu, cazul raportat în anul 2010 de WALL STREET JOURNAL, în care o rețea internațională de criminali a furat circa 70 milioane dolari de la mici firme, municipalități şi biserici, raportat în Verisign, *The domain name industry brief*, vol. 8, Iss. 3, August (2011).

[5] Contaminantul informatic Downadup a afectat rețeaua de calculatoare a Penitenciarului Rahova, rețeaua internă a IGPR şi rețeaua Tribunalului Bucureşti, rezultând în nefuncționarea sistemului ECRIS (sistemul informatic de management al dosarelor de judecată) – vezi detalii la http://www.mondonews.ro/Virusul-Downadup-a-atacat-mai-multe-institutii+id-7424.html. Sistemul municipal de justiție din Houston, Texas, a fost infectat de contaminanți informatici, rezultând în afectarea capacității de acțiune a poliției – vezi detalii la http://www.chron.com/disp/story.mpl/front/6250411.html.

[6] Vezi D. Barrett, *Hackers Penetrate Nasdaq Computers*, WALL STREET JOURNAL, February 5 (2011).

[7] Cazul Aurora, spre exemplu: în ianuarie 2010, un atac informatic asupra mai multor corporații globale, printre care Google, IBM, Microsoft şi Adobe, declanşat din China – vezi detalii în A. Boulanger şi S. Ghosh, *Malicious Code*, în S. Ghosh şi E. Turrini (eds.), *Cybercrimes: A Multidisciplinary Analysis* (2010); Symantec, *Global Internet Security Threat Report Trends for 2009*, Vol. XV, April (2010). Vezi şi cazurile Sony, Honda, Fox News, Epsilon şi Citibank, menționate în Kaspersky Lab, *IT Threat Evolution: Q2 2011*.

[8] Vezi McAfee, *Global Energy Cyberattacks: „Night Dragon"* (2011).

(vezi, spre exemplu, cazul atacului informatic asupra Estoniei)[1]. Impactul atacurilor informatice depinde de victimă şi poate consta în pagube financiare mari[2], încălcarea drepturilor de proprietate intelectuală, contaminarea sau copierea datelor informatice, blocarea accesului la date informatice, repudierea tranzacţiilor sau comunicaţiilor electronice, încetinirea vitezei de procesare a datelor ş.a. Pentru aceste motive, securitatea cyberspaţiului (*cybersecurity*), armonizarea legislaţiei şi cooperarea internaţională în acest domeniu sunt foarte importante, fapt reflectat, printre altele, de numeroase iniţiative legislative[3], Rezoluţii ale Naţiunilor Unite[4] sau ale Uniunii Internaţionale a Telecomunicaţiilor (ITU, agenţie a Naţiunilor Unite)[5] sau conferinţe internaţionale pe această temă[6].

Promovând o „cultură a securităţii" în societatea contemporană, Organizaţia pentru Cooperare şi Dezvoltare Economică (OECD)[7]

---

[1] Descris în M. Donner, *Cyberassault on Estonia*, IEEE SECURITY & PRIVACY, vol. 5, Iss. 4 (2007), p. 4; vezi şi G. Evron, *Battling botnets and online mobs: Estonia's defense efforts during the internet war*, GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS, 9(1), 121–126 (2008).

[2] Vezi numeroase studii pe această temă: JP Morgan Chase, *Cybercrime: The Growing Global Threat* (2011); Uniunea Europeană, http://ec.europa.eu/home-affairs/policies/crime/crime_cybercrime_en.htm (circa 750 miliarde euro anual); PricewaterhouseCoopers, *Global State of Information Security Survey* (2011); Ernts & Young, *Insights on IT risk*, April (2011); Interpol, *Financial and High-tech Crimes* (2009); United Nations Conference on Trade and Development, *Information Economy Report* (2005).

[3] Vezi, spre exemplu, The White House, Office of the Press Secretary, *Cybersecurity Legislative Proposal*, May 12 (2011).

[4] Vezi Rezoluţiile 56/121 - *Combating the criminal misuse of information technologies* (2002) şi 55/63 - *Combating the criminal misuse of information technologies* (2001).

[5] Vezi, spre exemplu, Rezoluţia 181 (Guadalajara, 2010) - *Definitions and terminology relating to building confidence and security in the use of information and communication technologies* şi Rezoluţia 130 - *Strengthening the role of ITU in building confidence and security in the use of information and communication technologies*.

[6] Vezi, spre exemplu, J. Vogel, *Towards a Global Convention against Cybercrime*, FIRST WORLD CONFERENCE OF PENAL LAW. Penal law in the XXI[st] century, Guadalajara, Mexic, 18-23 November (2007).

[7] Vezi OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002). Vezi şi United Nations General Assembly,

propune următoarele aspecte importante legate de securitatea sistemelor informatice:

I. **Conştientizare:** Participanții trebuie să fie conştienți de nevoia de securitate a sistemelor informatice şi de ce pot face pentru a îmbunătăți securitatea acestora.
II. **Responsabilitate:** Toți participanții sunt responsabili de securitatea sistemelor informatice.
III. **Răspuns:** Participanții trebuie să acționeze într-o manieră co-operativă şi rapidă pentru a preveni, detecta şi răspunde la incidentele de securitate.
IV. **Etică:** Participanții trebuie să respecte interesele legitime ale celorlalți.
V. **Democrație:** Securitatea sistemelor informatice trebuie să fie compatibilă cu valorile esențiale ale unei societăți democratice.
VI. **Evaluarea riscurilor:** Participanții trebuie să evalueze riscurile de securitate.
VII. **Design şi implementare a securității:** Participanții trebuie să încorporeze securitatea ca un element esențial al sistemelor informatice.
VIII. **Managementul securității**[1]**:** Participanții trebuie să adopte o abordare comprehensivă a managementului securității sistemelor informatice; managementul trebuie să se bazeze pe evaluarea riscurilor şi trebuie să fie dinamic, acoperind toate nivelurile de activitate a participanților şi toate aspectele operațiilor lor. Managementul trebuie să includă răspunsuri anticipative la amenințări emergente şi să adreseze prevenirea, detectarea şi răspunsul la incidente, recuperarea după disfuncționalități, întreținere şi audit. Politicile, practicile,

---

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (2010); United Nations, Resolution 58/199 - *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* (2004); United Nations, Resolution 57/239 - *Creation of a global culture of cybersecurity* (2003).

[1] Cele mai importante provocări pentru managementul securității sistemelor informatice în secolul al XXI-lea sunt considerate a fi: creşterea mobilității şi complexității, creşterea dimensiunii şi concentrării riscului, modificarea contextului şi incertitudinii majore, deplasarea responsabilităților şi importanța percepției riscului – vezi în OECD, *Emerging risks in the 21st century. An agenda for action* (2003).

măsurile şi procedurile de securitate trebuie coordonate şi integrate într-un sistem coerent. Cerinţele de securitate depind de nivelul de implicare a participanţilor, rolul acestora, riscul implicat şi cerinţele sistemului.

IX. **Reevaluare:** Deoarece noi ameninţări sau vulnerabilităţi pot să apară, participanţii trebuie să revadă şi să reevalueze securitatea sistemelor informatice şi să facă modificările necesare la nivel de politici, practici, măsuri şi proceduri.

Cartea de faţă abordează în mod holistic criminalitatea în cyberspaţiu şi contribuie la dezvoltarea unei înţelegeri complete şi efective a acesteia şi a principalelor mijloace de prevenire a ei. Cartea este structurată în trei părţi: Partea I prezintă componentele şi caracteristicile sistemelor informatice şi ale Internetului, urmate de cerinţele operaţionale şi legale de securitate şi ameninţările prezente la adresa sistemelor informatice; Partea a II-a prezintă mijloace legale de prevenire a criminalităţii în cyberspaţiu; Partea a III-a prezintă mijloace procedurale şi tehnice de prevenire a criminalităţii în cyberspaţiu.

Abordarea cercetării pentru această carte a fost interdisciplinară, o tendinţă modernă în domeniul dreptului[1] şi al sistemelor informatice[2]. Pentru elaborarea acestei cărţi a fost realizat un studiu exhaustiv al literaturii relevante. Formalizarea politicilor şi procedurilor de securitate ale sistemelor informatice se bazează pe cercetare empirică.

Considerăm că această carte se va dovedi foarte utilă juriştilor, managerilor sistemelor informatice, organelor judiciare, cadrelor didactice universitare, studenţilor de la facultăţi de drept, afaceri sau informatică, cercetătorilor, tuturor celor interesaţi de domeniul sistemelor informatice în general şi fiecărui utilizator de calculatoare pentru a înţelege ameninţările informatice, impactul lor potenţial şi măsurile necesare pentru protejarea personală.

---

[1] Vezi J. Palfrey, *The Challenge of Developing Effective Public Policy on the Use of Social Media by Youth*, FEDERAL COMMUNICATIONS LAW JOURNAL, vol. 63 (2010); D. W. Vic, *Interdisciplinarity and the Discipline of Law*, JOURNAL OF LAW AND SOCIETY, Vol. 31, No. 2, June, 163-193 (2004).

[2] Vezi, spre exemplu, I. Benbasat şi R. W. Zmud, *The identity crisis within the IS discipline: Defining and communicating the discipline's core properties*, MIS QUARTERLY, 27 (2), 183–194 (2003); R. D. Galliers, *Trans-disciplinary research in information systems*, INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT, 24, 99-106 (2004).

Partea I

CYBERSPAŢIU

1. SISTEME INFORMATICE

1.1. Definiţie

Cyberspaţiul este domeniul global în mediul informaţional constând din reţeaua interdependentă de infrastructuri informatice incluzând Internet, reţelele de comunicaţii electronice, sistemele informatice şi procesoarele şi controlerele încorporate[1]. *Reţea de comunicaţii electronice* înseamnă sisteme de transmisie şi, după caz, echipamente de comutare sau de rutare şi alte resurse, inclusiv elemente de reţea care nu sunt active, care permit transmiterea semnalelor prin cablu, unde radio, prin mijloace optice sau prin alte mijloace electromagnetice, inclusiv reţele de satelit, reţele terestre fixe (cu comutare de circuite sau de pachete, inclusiv Internet) şi mobile, sisteme care utilizează reţeaua electrică, atât timp cât servesc la transmiterea semnalelor, reţelele utilizate pentru difuzarea programelor de radio şi televiziune şi reţelele de televiziune prin cablu, indiferent de tipul de informaţie transmisă[2]. *Reţea publică de comunicaţii* înseamnă o reţea de comunicaţii electronice utilizată în întregime sau în principal pentru furnizarea de servicii de comunicaţii electronice puse la dispoziţia publicului, care asigură transferul de informaţii între punctele de terminale ale reţelei[3].

În general, sistemele pot fi identificate ca fiind:

- *Simple*: constând din puţine variabile, cu relaţii lineare între ele, care pot fi descrise, explicate şi prezise cu precizie;

---

[1] Vezi NIST, *Managing Information Security Risk: Organization, Mission, and Information System View* (2011).

[2] Vezi Directiva 2009/140/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009, de modificare a Directivelor 2002/21/CE privind un cadru de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice, 2002/19/CE privind accesul la reţelele de comunicaţii electronice şi la infrastructura asociată, precum şi interconectarea acestora şi 2002/20/CE privind autorizarea reţelelor şi serviciilor de comunicaţii electronice; vezi şi Legea nr. 527 din 17 iulie 2002.

[3] *Id.*

- *Complicate*: constând din multe variabile, într-un sistem închis cu relaţii lineare şi non-lineare, care pot fi descrise, explicate şi prezise cu precizie; sau
- *Complexe*: constând din multe variabile, într-un sistem deschis cu relaţii non-lineare, care nu pot fi descrise, explicate şi prezise cu precizie.

După cum argumentează unii cercetători[1], caracteristicile sistemelor *complexe* includ:

- Numărul mare de elemente, care fac dificilă înţelegerea lor completă;
- Existenţa unor interacţiuni dinamice între elemente şi transferul de informaţii;
- Natura bogată şi multidimensională a interacţiunilor între elemente;
- Caracterul nonlinear al interacţiunilor, care poate cauza reacţii extinse;
- Existenţa feedback-ului pozitiv şi negativ recurent în sistem;
- Deschiderea către alte sisteme, influenţate de mediul lor şi de observatori;
- Elementele componente sunt simple, complexitatea sistemului rezultând din natura interacţiunilor între elemente.

O clasificare a *sistemelor deschise* poate fi găsită în Falkenberg şi colab.[2], unde se disting următoarele tipuri de sisteme:

- *Sistem reactiv*: fiecare expresie este o reacţie, iar fiecare impresie cauzează o reacţie.
- *Sistem responsiv*: pentru fiecare expresie o anumită impresie sau pattern temporal este o condiţie necesară, dar nu suficientă pentru a determina apariţia expresiei.
- *Sistem autonom*: cel puţin o expresie este o acţiune.

---

[1] Vezi, spre exemplu, P. Cilliers, *Complexity and Postmodernism*, Routledge (1998); K. Richardson şi P. Cilliers, *What Is Complexity Science?: A View from Different Directions*, EMERGENCE, 3 (1) 5-23 (2001).

[2] Vezi E. D. Falkenberg, W. Hesse, P. Lindgreen, B. E. Nilsson, J. L. H. Oei, C. Rolland, R. K. Stamper, F. J. M. Van Assche, A. A. Verrijn-Stuart şi K. Voss, *A framework of information system concepts*, The FRISCO Report (1998).