

Cuprins

Mulțumiri	5
Abrevieri.....	7
Considerații introductive.....	9
PARTEA I. ASPECTE GENERALE PRIVIND SECURITATEA SISTEMELOR INFORMATICE ȘI CRIMINALITATEA INFORMATICĂ.....	11
Capitolul I. Amenințări și tendințe în ce privește securitatea sistemelor informatice și rețelelor de comunicații.....	13
<i>Secțiunea I. Considerații generale</i>	<i>13</i>
<i>Secțiunea a II-a. Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații.....</i>	<i>13</i>
§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice	15
§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor.....	18
§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare	22
§ 4. Lough Daniel Lawry, O taxonomie a atacurilor asupra calculatoarelor cu aplicație pentru rețelele fără fir	25
§ 5. RAND Europe, O taxonomie a incidentelor de securitate	26
Capitolul II. Conceptul, principalele caracteristici și evoluția criminalității informatice	29
<i>Secțiunea I. Considerații generale</i>	<i>29</i>
<i>Secțiunea a II-a. Conceptul „criminalitate informatică”</i>	<i>29</i>
§ 1. Noțiunea de criminalitate.....	29
§ 2. Noțiunea de criminalitate informatică	30
§ 3. Infrațiuni din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	32
<i>Secțiunea a III-a. Principalele caracteristici ale criminalității informatice</i>	<i>34</i>
<i>Secțiunea a IV-a. Aspecte privind evoluția criminalității informatice</i>	<i>35</i>
§ 1. Etapele evoluției.....	35
§ 2. Amenințări actuale	36
§ 3. Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului	37

3.1. Dependența de tehnologia informației și comunicațiilor	37
3.2. Numărul utilizatorilor	37
3.3. Disponibilitatea dispozitivelor și accesului	38
3.4. Disponibilitatea informațiilor	39
3.5. Lipsa mecanismelor de control	39
3.6. Dimensiunile internaționale	39
3.7. Independența locației și prezenței la locul infracțiunii	40
3.8. Automatizarea	40
3.9. Resursele	41
3.10. Viteza proceselor de schimb de date	42
3.11. Viteza de dezvoltare	42
3.12. Comunicațiile anonime	42
3.13. Tehnologia de criptare	43
§ 4. Particularități ale evoluției fenomenului criminalității informatic în România	44
4.1. Repere temporale	44
4.2. Particularități	45

Capitolul III. Explicații criminologice ale subculturilor

criminalității informatice	51
<i>Secțiunea I. Considerații generale</i>	51
<i>Secțiunea a II-a. O scurtă prezentare a Teoriei lui Emile Durkheim</i>	51
<i>Secțiunea a III-a. O scurtă prezentare a Teoriei lui Robert Merton</i>	52
<i>Secțiunea a IV-a. Explicarea subculturilor criminalității informatice prin prisma tipologiei modurilor individuale de adaptare dezvoltată de Merton</i>	54
§ 1. Conformismul navigatorilor pe Internet	56
§ 2. Inovația: hacking-ul pentru profit	56
§ 3. Ritualismul: hacking-ul ca obișnuință	57
§ 4. Retragerea: hacking-ul ca dependență	57
§ 5. Rebeliunea: hacking-ul ca nesupunere la regulile societății	57
§ 6. Hackingul non-utilitar	58

PARTEA A II-A. PREOCUPĂRI ALE SOCIETĂȚII INTERNAȚIONALE PENTRU PREVENIREA ȘI COMBATerea CRIMINALITĂȚII INFORMATICE

59

Capitolul I. Organizații internaționale și regionale cu atribuții și preocupări în prevenirea și combaterea criminalității informatice și principalele realizări

61

<i>Secțiunea I. Considerații generale</i>	61
---	----

Secțiunea a II-a. Organizația Națiunilor Unite (UN)	61
Secțiunea a III-a. Grupul celor Șapte Națiuni (G7)	66
Secțiunea a IV-a. Uniunea Internațională a Telecomunicațiilor (ITU).....	70
Secțiunea a V-a. Consiliul Europei (CoE)	73
Secțiunea a VI-a. Uniunea Europeană (EU).....	76

Capitolul II. Principalele instrumente juridice și recomandări cu vocație internațională și regională care conțin reglementări privind prevenirea și combaterea criminalității informatice	79
<i>Secțiunea I. Considerații generale</i>	<i>79</i>
<i>Secțiunea a II-a. Recomandarea nr. R (89) 9 asupra criminalității în relație cu calculatorul</i>	<i>81</i>
<i>Secțiunea a III-a. Convenția privind criminalitatea informatică</i>	<i>83</i>
<i>Secțiunea a IV-a. Protocolul adițional referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice.....</i>	<i>86</i>

Capitolul III. Analiză comparativă a modului în care legislatorii naționali au implementat măsurile prevăzute de Convenția privind criminalitatea informatică	89
<i>Secțiunea I. Considerații generale</i>	<i>89</i>
<i>Secțiunea a II-a. Analiza comparativă a modului în care au fost definiți termenii utilizați.....</i>	<i>90</i>
<i>Secțiunea a III-a. Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității și disponibilității datelor</i>	<i>92</i>
§ 1. Accesarea ilegală	93
§ 2. Interceptarea ilegală.....	96
§ 3. Afectarea integrității datelor	99
§ 4. Afectarea integrității sistemului.....	101
§ 5. Abuzurile asupra dispozitivelor	102
<i>Secțiunea a IV-a. Analiza comparativă a modului în care au fost incriminate infracțiunile informatice</i>	<i>105</i>
§ 1. Falsificarea informatică.....	105
§ 2. Frauda informatică.....	108
<i>Secțiunea a V-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la conținut.....</i>	<i>110</i>
§ 1. Infracțiuni referitoare la pornografia infantilă.....	110

<i>Secțiunea a VI-a. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe.....</i>	114
---	-----

Capitolul IV. Puncte de vedere exprimate în literatura și doctrina de specialitate cu privire la metodele, tehnicile și procedurile de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	120
<i>Secțiunea I. Considerații generale.....</i>	120
<i>Secțiunea a II-a. Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) prezentate în literatura de specialitate</i>	120
§ 1. Pollit M. Mark, Paradigma digitală.....	121
§ 2. Farmer Dan, Venema Wietse, Analiza criminalistică a computerelor UNIX	122
§ 3. Primul Atelier de lucru de cercetare criminalistică digitală (DFRWS), Procesul de investigație în raport cu știința criminalistică digitală.....	122
§ 4. Reith Mark, Carr Clint, Gunsch Gregg, Un model criminalistic digital abstract.....	125
§ 5. Gordon R. Gary, Hosmer D. Chet, Siedma Christine, Rebovich Dan, Metodologia investigării criminalistice digitale.....	126
§ 6. Carrier Brian, Spafford H. Eugene, Un proces integrat de investigație digitală	128
§ 7. Baryamureeba Venansuis, Tushabe Florence, Un model avansat/îmbunătățit al procesului integrat de investigare digitală.....	129
§ 8. Ciardhuain O´ Séamus, Un model extins de investigații a criminalității informatice.....	130
§ 9. Kohn Michael, Elloff JHP, Oliver MS, Model cadru pentru investigarea criminalistică digitală	131
§ 10. Freiling C. Felix, Schwittay Bastian, Un model comun procesului pentru răspuns la incident și investigare criminalistică digitală.....	132
<i>Secțiunea a III-a. Principalele proceduri, ghiduri, practici dezvoltate în domeniul prevenirii și combaterii criminalității informatice</i>	134
§ 1. Organizația Națiunilor Unite, Manual pentru prevenirea și controlul infracțiunilor în legătură cu calculatorul.....	135
§ 2. INTERPOL, Manualul de Investigare a Infracțiunilor privind Tehnologia Informațiilor (ITCIM).....	137

§ 3. Rețeaua Europeană a Institutelor de Criminalistică (ENFSI) Orientări pentru bune practici în examinarea criminalistică a tehnologiilor digitale.....	138
§ 4. Compartimentul pentru Criminalitate Informatică și Proprietate Intelectuală din cadrul Direcției Penale a Ministerului de Justiție al SUA, Punerea sub acuzare a infracțiunilor din sfera criminalității informatice	140
§ 5. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Investigarea scenei „electronice” a infracțiunii: Un ghid pentru primul respondent.....	142
§ 6. Serviciul Secret al SUA, Bune practici pentru confiscarea dovezilor electronice: Un ghid de buzunar pentru prim-respondent	144
§ 7. Asociația Ofițerilor Șefi ai poliției din Anglia, Țara Galilor și Irlanda de Nord, Ghid de bune practici pentru dovezi electronice din (bazate pe) calculator	147
§ 8. Institutul Național de Justiție din cadrul Ministerului de Justiție al SUA, Examinarea criminalistică a dovezilor digitale: un ghid pentru autoritățile de aplicare a legii.....	148
§ 9. Compartimentul pentru Criminalitate, Informatică și Proprietate Intelectuale din cadrul Direcției penale a Ministerului de Justiție al SUA, Căutarea și confiscarea calculatoarelor și obținerea dovezilor electronice în investigațiile penale.....	150
§ 10. Institutul Național pentru Standarde și tehnologie din cadrul Ministerului Comerțului al SUA, Ghid pentru gestionarea incidentelor de securitate a calculatoarelor.....	151

PARTEA A III-A. COORDONATELE ACTIVITĂȚII ORGANELOR LEGISLATIVE ȘI EXECUTIVE DIN ROMÂNIA PENTRU DEZVOLTAREA CONCEPTULUI DE PREVENIRE ȘI COMBATERE A CRIMINALITĂȚII INFORMATICE 157

Capitolul I. Prevenirea criminalității informatice	159
<i>Secțiunea I. Considerații generale privind prevenirea criminalității.....</i>	159
<i>Secțiunea a II-a. Măsuri specifice de prevenire a criminalității informatice.....</i>	160

Capitolul II. Incriminarea faptelor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	162
<i>Secțiunea I. Considerații generale</i>	162

<i>Secțiunea a II-a. Analiza conținutului normelor de incriminare a faptelor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	162
§ 1. Accesul ilegal la un sistem informatic.....	163
§ 2. Interceptarea ilegală a unei transmisii de date informatice.....	166
§ 3. Alterarea integrității datelor informatice	169
§ 4. Perturbarea funcționării sistemelor informatice	172
§ 5. Transferul neautorizat de date informatice.....	175
§ 6. Operațiuni ilegale cu dispozitive sau programe informatice	178
§ 7. Falsul informatic	182
§ 8. Frauda informatică.....	184
Capitolul III. Particularități ale percheziției informatice.....	188
§ 1. Considerații generale	188
§ 2. Reglementarea percheziției informatice	189
2.1. Percheziția informatică în reglementarea anterior în vigoare	189
2.2. Percheziția informatică în reglementarea în vigoare	189
§ 3. Încuviințarea percheziției informatice.....	190
3.1. Organele judiciare competente să dispună percheziția informatică	190
3.2. Persoanele care pot solicita încuviințarea percheziției informatice	190
3.3. Motive pentru a solicita încuviințarea percheziției informatice	191
3.4. Condiții pentru a solicita încuviințarea percheziției informatice	191
3.5. Elaborarea și înaintarea cererii de încuviințare a percheziției informatice	192
3.6. Soluționarea cererii de încuviințare a percheziției informatice	193
3.7. Emiterea mandatului de percheziție informatică	194
§ 4. Efectuarea percheziției informatice	195
4.1. Persoanele abilitate să efectueze percheziția informatică.....	195
4.2. Alte persoane în prezența cărora se efectuează percheziția informatică	195
4.3. Perioada în care poate fi efectuată percheziția informatică.....	196
4.4. Mijloace tehnice și proceduri folosite pentru efectuarea percheziției informatice	197
4.5. Activități prealabile efectuării percheziției informatice	197

4.6. Colectarea datelor informatice, cu ocazia percheziției informatice.....	198
4.7. Examinarea datelor informatice colectate, cu ocazia efectuării percheziției informatice	202
4.8. Întocmirea procesului-verbal de percheziție informatică.....	203
4.9. Asigurarea confidențialității datelor/informațiilor cunoscute cu ocazia percheziției informatice	204
Capitolul IV. Instituții cu atribuții în prevenirea și combaterea criminalității informatice și principalele realizări	205
<i>Secțiunea I. Considerații generale</i>	<i>205</i>
<i>Secțiunea a II-a. Structura specializată în cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție</i>	<i>205</i>
§ 1. Structura Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism.....	205
§ 2. Structura Secției de combatere a infracțiunilor de terorism și a criminalității informatice.....	206
§ 3. Rolul Serviciului de combatere a criminalității informatice și atribuțiile procurorilor din cadrul acestuia.....	207
3.1. Rolul Serviciului de combatere a criminalității informatice.....	207
3.2. Atribuțiile procurorilor din cadrul Serviciului de combatere a criminalității informatice.....	207
<i>Secțiunea a III-a. Structura specializată în cadrul Inspectoratului General al Poliției Române.....</i>	<i>208</i>
§ 1. Structura Direcției de Combatere a Criminalității Organizate.....	209
§ 2. Structura Serviciului de combatere a criminalității informatice și atribuțiile polițiștilor din cadrul acestuia.....	209
2.1. Structura Serviciului de combatere a criminalității informatice	209
2.2. Atribuțiile polițiștilor din cadrul Serviciului de combatere a criminalității informatice.....	210
<i>Secțiunea a IV-a. Principalele realizări pe linia combaterii criminalității informatice.....</i>	<i>210</i>
§ 1. Repere statistice	210
§ 2. Cauze instrumentate.....	213
Capitolul V. Cooperarea internațională pentru prevenirea și combaterea criminalității informatice	219

PARTEA A IV-A. PUNCTE DE VEDERE CU PRIVIRE LA METODOLOGIA CERCETĂRII INFRAȚIUNILOR DIN SFERA CRIMINALITĂȚII INFORMATICE/LA REGIMUL TEHNOLOGIEI INFORMAȚIEI ȘI COMUNICAȚIILOR (TIC)	223
---	------------

Capitolul I. Conceptul investigare criminalistică digitală, status-ul și conținutul acestui proces	225
<i>Secțiunea I. Conceptul investigare criminalistică digitală</i>	<i>225</i>
<i>Secțiunea a II-a. Status-ul și conținutul procesului de investigare criminalistică digitală</i>	<i>226</i>

Capitolul II. Considerații generale cu privire la metodologia cercetării infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	229
<i>Secțiunea I. Clasic și nou în cercetarea infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>229</i>
<i>Secțiunea a II-a. Principiile, scopul și definiția metodologiei de cercetare a infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>230</i>
§ 1. Precizări terminologice cu privire la cercetarea penală a infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și investigarea criminalistică a locului faptei și a sistemelor informatice	230
§ 2. Principiile cercetării infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și investigării criminalistice a locului faptei și a sistemelor informatice	231
2.1. Principiile cercetării infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	231
2.2. Principiile investigării criminalistice a locului faptei și a sistemelor informatice	232
§ 3. Obiectivele cercetării infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	232
3.1. Obiectivul cercetării penale a infrațunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)	232

3.2. Obiectivul investigării criminalistice a locului faptei și a sistemelor informatice	233
3.3. Obiectivele concrete ale cercetării infracțiunilor din sfera criminalității informatice.....	233
§ 4. Definiția metodologiei cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC).....	234

Capitolul III. Formalizarea și standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)

<i>Secțiunea I. Considerații generale</i>	235
<i>Secțiunea a II-a. Necesitatea standardizării activității de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC), de acreditare a laboratoarelor criminalistice și de certificare a specialiștilor și a mijloacelor de investigare.....</i>	235
<i>Secțiunea a III-a. Perspective actuale privind standardizarea activității de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și acreditarea laboratoarelor criminalistice</i>	236
§ 1. Situația la nivel internațional	236
1.1. În domeniul standardizării	236
1.2. În domeniul acreditării.....	237
§ 2. Situația la nivel european.....	238
2.1. În domeniul standardizării	238
2.2. În domeniul acreditării.....	238
2.3. În domeniul evaluării conformității.....	238
În domeniul evaluării conformității, la nivel european, organismul competent este Sistemul European de Testare, Inspecție și Certificare (ETICS), o asociație non-profit, care are ca scop administrarea sistemului ENEC și a altor sisteme de evaluare a conformității, cum ar fi CCA, HAR și LOVAG, evaluând conformitatea produselor cu terți, în principal în sectorul electrotehnic (dar și în alte domenii care pot fi asociate cu testarea, inspecția și certificarea produselor, proceselor și personalului).	238
§ 3. Situația în SUA	239

3.1. În domeniul standardizării.....	239
3.2. În domeniul acreditării	239
3.3. În domeniul evaluării conformității	239
§ 4. Situația în România.....	240
4.1. În domeniul standardizării.....	240
4.2. În domeniul acreditării	241
Capitolul IV. Procedura cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) propusă	243
<i>Secțiunea 1. Necesitatea modificării/completării procedurilor de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC)</i>	<i>243</i>
<i>Secțiunea a II-a. Etapele/fazele cercetării infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) propuse</i>	<i>244</i>
§ 1. Activitățile premergătoare cercetării propriu-zise	245
§ 2. Cercetarea la fața locului	245
§ 3. Efectuarea perchezițiilor (informatice, domiciliară, altele)	246
§ 4. Ascultarea persoanelor (suspecți, martori, persoane vătămate).....	246
§ 5. Examinarea dovezilor	247
§ 6. Finalizarea cercetărilor	247
<i>Secțiunea a III-a. Aspecte privind conținutul și forma de redactare a procedurii/procedurilor.....</i>	<i>249</i>
<i>Secțiunea a IV-a. Particularitățile unor activități de cercetare a infracțiunilor din sfera criminalității informatice/la regimul tehnologiei informației și comunicațiilor (TIC) și de investigare criminalistică a locului faptei și a sistemelor informatice.....</i>	<i>250</i>
§ 1. Particularități ale pregătirii cercetării/investigației	250
§ 2. Particularități ale căutării/conservării dovezilor materiale/digitale	251
§ 3. Particularități privind informațiile care trebuie furnizate de/obținute de la suspecți/inculpați, martori, persoane vătămate	253
3.1. Posibile întrebări cu caracter general	253
3.2. Posibile întrebări cu caracter particular	254
§ 4. Particularități ale dovezilor digitale.....	257
§ 5. Particularități ale colectării dovezilor digitale	258
§ 6. Particularități ale examinării dovezilor digitale	258

§ 7. Particularități ale documentării cercetării și întocmirii rapoartelor (de constatare tehnico-științifică/expertiză)	259
§ 8. Particularități ale echipamentelor (hardware) și programelor (software) specializate folosite în investigarea criminalistică digitală.....	260
Scurte concluzii și propuneri	262
Bibliografie selectivă.....	267

Capitolul I

Amenințări și tendințe în ce privește securitatea sistemelor informatice și rețelelor de comunicații

Secțiunea I

Considerații generale

Încă de la apariția sistemelor informatice și rețelelor de comunicații au fost căutate vulnerabilitățile acestora, fie în scopul îmbunătățirii performanțelor și siguranței în exploatare fie în scopul compromiterii lor.

Secțiunea a II-a

Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații

Taxonomia, conform definiției¹, este mai mult decât o clasificare, în sensul că aceasta descrie principiile conform cărora clasificarea a fost făcută, dar și procedura care trebuie urmată pentru clasificarea unui obiect nou².

În sfera securității sistemelor informatice și a rețelelor de comunicații, taxonomiile au apărut din nevoia de a oferi consecvență și coerență în limbajul utilizat pentru descrierea și clasificarea vulnerabilităților și atacurilor asupra acestora și a se evita astfel (pe cât posibil) confuziile.

De asemenea, aceste taxonomii permit aplicarea cunoștințelor anterioare amenințărilor noi, cât și un mod organizat de percepere a acestora (amenințărilor).

O taxonomie satisfăcătoare prezintă următoarele caracteristici³:

¹ Taxonomia este considerată „știința legilor de clasificare” (a se vedea Academia Română Institutul de lingvistică, Iorgu Iordan, *Dicționar explicativ al limbii române*, ed. a II-a, Ed. Univers Enciclopedic, București, 1998, p. 1072) sau „știința care se ocupă cu stabilirea legilor de clasificare și sistematizare a domeniilor din realitate cu o structură complexă” (a se vedea DEX online, la <http://dexonline.ro/search.php?Cuv=taxonomie>).

² A se vedea și Berghes C. V., Riordan J. Piessens F., *A Vulnerability Taxonomy Methodology applied to web Services*, L.P. 4, disponibil on-line la http://chris.vandenberghes.org/publications/vulnerability_taxonomy_nerdsec2005.pdf.

³ Lough D. L., *A Taxonomy of Computer Attack with Application to Wireless Networks*, teză de doctorat susținută la Virginia Polytechnic Institute and State University, Virginia, (apr.), 2001, p. 37-39, disponibil on-line la <http://scholar.lib.vt.edu/theses/available/etd-04252001->

- **acceptată** (Howard, 1997)/**adecvată** (Amoroso, 1994), în sensul de a fi structurată de o asemenea manieră astfel încât să fie aprobată în general;
- **comprehensibilă** (Lindqvist și Jonsson, 1997), în sensul de a putea fi înțeleasă atât de către specialiști, cât și de către cei care manifestă interes în domeniu;
- **completă** (Amoroso, 1994)/**exhaustivă** (Howard, 1997; Lindqvist și Jonson, 1997), în sensul că ar trebui să țină cont de toate posibilele amenințări;
- **precisă** (Krsul, 1998; Bishop, 1999)/**clară** (Howard, 1997; Lindqvist și Jonsson, 1997), în sensul că trebuie să fie clar precizată astfel încât să evite ambiguitatea;
- **repetabilă** (Howard, 1997; Lindqvist și Jonsson, 1997), în sensul că acele clasificări ar trebui să fie repetabile;
- **folositoare** (Howard, 1997; Lindqvist și Jonsson, 1997), în sensul că trebuie să poată fi utilizată pentru o bună cunoaștere a domeniului;
- **obiectivă** (Krsul, 1998), în sensul că acele caracteristici trebuie să fie identificate de la obiectul cunoscut nu de la cunoștințele subiectului;
- **să se excludă reciproc** (Howard, 1997; Lindqvist și Jonsson, 1997), în sensul că o anumită amenințare să fie grupată într-o singură categorie.

*Față de caracteristicile prezentate, se poate concluziona*¹:

- realizarea unei bune taxonomii este dificilă;
- taxonomia depinde nu numai de amenințările respective ci și de punctul de vedere a celui care o realizează, punct de vedere care este condiționat de presupusa utilizare a taxonomiei;
- amenințările, frecvent, se manifestă grupat și prezintă proprietăți comune.

Din motivele prezentate, nu surprinde marea diversitate a taxonomiilor dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații.

Având în vedere că majoritatea acestor taxonomii au un pronunțat caracter tehnic, de specialitate, fiind dezvoltate de specialiștii din domeniul securității sistemelor informatice și rețelelor de comunicații și mai puțin pentru autoritățile de aplicare a legii, am să prezint în continuare acele taxonomii înțelese și de aceia

234145/unrestricted/lough.dissertation.pdf. Lough compilează proprietățile unei taxonomii din lucrările a cinci autori Amoroso E. G. (*Fundamentals of Computer Security Technology*, Prentice Hall, Englewood Cliffs, N.J., 1994), Bishop M. (*How Attackers Break Programs, and How to Write Programs More Securely*, 8th net, USENIX Security Symposium, aug., 1999), Howard J. D. (*An Analysis of Security Incident on the Internet*, 1989-1995, teză de doctorat susținută la Purdue University, apr., 1997), Krsul I. V. (*Software Vulnerability Analysis*, teză de doctorat susținută la Purdue University, mai, 1998) Lindqvist U. și Johnsson E., (*How to Systematically Classify Computer Security Intrusions*, IEEE Security and Privacy, 1997).

¹ A se vedea și Berghe C.V., Riordan J., Piessens F., *A Vulnerability ...*, op. cit., p. 5.

care nu sunt neapărat specialiști, dar manifestă interes în domeniul securității sistemelor informatice și rețelelor.

§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice¹

Această taxonomie (numită de autori, din modestie, clasificare) este bazată atât pe clasificările anterioare cât și pe experiența autorilor.

Autorii consideră că fiecare *atac* întrunește **14 trăsături**² care sunt prezentate schematic și în legătură³:

(1) *în funcție de obiectivul atacului:*

- (1.1) dobândirea privilegiului administratorului (super-utilizatorului);
- (1.2) dobândirea privilegiului utilizatorului;
- (1.3) refuzarea serviciului;
- (1.4) încălcarea serviciului;
- (1.5) încălcarea confidențialității informațiilor sau resurselor sistemului;
- (1.6) executarea codurilor malițioase;
- (1.7) încălcarea politicii de securitate.

(2) *în funcție de tipul efectului:*

- (2.1) detectarea Codului executabil;
- (2.2) „Cal troian”, virus;
- (2.3) detectarea Codului executabil al aplicațiilor de (web) rețea;
- (2.4) utilizarea neautorizată a unei stații de lucru intermediare tip „server Proxy”;
- (2.5) inundarea memoriei tampon;
- (2.6) sondarea sau scanarea;
- (2.7) folosirea unor protocoale neacceptate;
- (2.8) folosirea unor porturi neacceptate;
- (2.9) deghizarea ca alt sistem „gazdă”;
- (2.10) inserarea unor obiecte false.

(3) *în funcție de nivelul modelului de referință ISO/OSI*

¹ Palauskas N., Garsva E., *Computer System Attack Classification*, în *Electronics and Electrical Engineering*, nr. 2 (66), 2006, pp. 84-87, disponibil on-line la <http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf>.

² *Ibidem*, p. 85.

³ *Ibidem*, p. 86.

- (3.1) fizic;
 - (3.2) conexiuni de date;
 - (3.3) rețea;
 - (3.4) transport;
 - (3.5) sesiune;
 - (3.6) prezentare;
 - (3.7) aplicație.
- (4) *în funcție de sistemul de operare OS*
- (4.1) Windows;
 - (4.2) Linux;
 - (4.3) Solaris;
 - (4.4) BSD;
 - (4.5) MacOS;
 - (4.6) altele.
- (5) *în funcție de locația subiectului atacului*
- (5.1) în interiorul segmentului local;
 - (5.2) între segmente;
 - (5.3) acces fizic;
 - (5.4) privilegiu de utilizator al sistemului;
 - (5.5) privilegiu de administrator de sistem.
- (6) *în funcție de tipul locației obiectului*
- (6.1) sistem local;
 - (6.2) rețea locală;
 - (6.3) rețea globală;
 - (6.4) rețea fără fir;
 - (6.5) rețea tip P2P.
- (7) *în funcție de serviciul atacat*
- (7.1) rețeaua (web), (HTTP);
 - (7.2) transfer de fișiere (FTP,SMB,CIFS);
 - (7.3) poștă (SMTP, POP 3, IMAP);
 - (7.4) control de rețea (SNMP);
 - (7.5) nume de domeniu (DNS);
 - (7.6) control la distanță (telnet, SSH, RDP);
 - (7.7) configurarea sistemului tip „Gazdă”;
 - (7.8) rutare dinamică (RIP, OSPF);
 - (7.9) incryptare (SSL);
 - (7.10) altele.
- (8) *în funcție de concentrarea atacului*
- (8.1) atomic;
 - (8.2) fragmentat.

- (9) *în funcție de retroacțiune*
 - (9.1) cu retroacțiune;
 - (9.2) fără retroacțiune.
- (10) *în funcție de condițiile inițiale de executare a atacului*
 - (10.1) la solicitarea obiectului de atac;
 - (10.2) la un eveniment specific obiectului de atac;
 - (10.3) necondiționat.
- (11) *în funcție de condițiile inițiale de executare a atacului*
 - (11.1) pasiv;
 - (11.2) activ.
- (12) *în funcție de automatizarea atacului*
 - (12.1) automat;
 - 12.2 semi-automat;
 - 12.3 manual.
- (13) *în funcție de sursa atacului*
 - (13.1) unu contra unu;
 - (13.2) mai mulți contra unu;
 - (13.3) unu contra mai mulți.
- (14) *în funcție de calitatea legăturilor*
 - (14.1) singură;
 - (14.2) multiplă.

Autorii consideră¹ (și de aici se conturează caracterul de taxonomie) că „realizarea obiectivului este cea mai importantă pentru atacator (1), prin urmare, evaluarea numerică a severității atacului este fondată pe aceasta. Tipul efectului (2) depinde mai mult de obiectivul intrusului la fel ca și locația subiectului și obiectului. Modelul ISO/OSI poate descrie toate procesele de sistem. Nivelul aplicației (3.7) este cel mai potrivit, din cauza potențialității și complexității sale, pentru a efectua atacuri. Există o varietate de sisteme de operare OS în rețeaua globală, familii specifice de sisteme de operare OS au vulnerabilități comune care atrag atacuri specifice OS (4). Locația subiectului atacului (5) influențează tipul efectului și probabilitatea îndeplinirii obiectului atacului. Tehnologia atacului și posibilele amenințări sunt influențate de tipul locației obiectului (6) și de serviciul atacat (7). Atacul poate fi concentrat într-un singur pachet, și atacul este denumit atomic (8.1.) sau poate fi fragmentat în câteva pachete (8.2.). Retroacțiunea (9) nu este necesară pentru toate atacurile... Pentru a evita detectarea sau pentru o mai bună eficiență, atacatorii pot alege diferite condiții inițiale de exe-

¹ *Ibidem*, p. 85.

cutare (10), tipuri de impact (11) sau nivele de automatizare (12). În conformitate cu obiectivele atacului și tipul efectului, numărul surselor atacului (13) și cantitatea legăturilor (14) pot diferi”.

§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor¹

Aceasta este una dintre cele mai bune taxonomii dezvoltate, și are ca bază teza de doctorat a lui John Howard (unul dintre autori), „*O analiză a incidentelor de securitate pe Internet 1989-1995*”².

Autorii au dezvoltat un set minim de termeni de „nivel înalt”, împreună cu o structură care indică legăturile dintre aceștia (o taxonomie), care poate fi folosită pentru a clasifica și înțelege informațiile incidentelor de securitate a calculatoarelor.

Unii autori susțin³ „Howard încearcă să concentreze atenția pe procesul care conduce taxonomia, mai degrabă, decât pe o schemă de clasificare... Aceasta înseamnă că întregul proces al atacului este luat în considerare, ceea ce este, cu siguranță, valoros... Howard nu reușește să îndeplinească una dintre cerințele taxonomiei sale: să se excludă reciproc. Unele dintre categorii se pot suprapune... pentru organele de informare cum ar fi CERT, o astfel de taxonomie nu poate fi practică. Organele de informare sunt mai preocupate de atacul în sine decât de motivațiile și obiectivele din spatele lui... problemele menționate mai sus există încă chiar cu taxonomia perfecționată”.

Nu sunt de acord cu aceste considerații și chiar dacă unele dintre subcategoriile descrise nu s-ar exclude reciproc, așa cum susțin autorii mai sus citați⁴ dar și alții⁵, *consider mai valoroasă descrierea procesului prin care atacatorul reușește să își îndeplinească obiectivul, decât o simplă clasificare a atacurilor.*

¹ Howard J.D., Longstaff T.A., *A Common Language for Computer Security Incidents*, Sandia Report (SAND98-8667), (oct.) 1998, disponibil on-line la http://www.cert.org/research/taxonomy_988667.pdf.

² Howard J.D., *An Analysis of Security Incidents on the Internet 1989-1995*, teză de doctorat susținută la Carnegie University, Pittsburg, Pennsylvania, (apr.) 1997, disponibil on-line la <http://www.dtic.mil/mil/cgi-bin/GetTRDoc?AD=ADA389085&Location=U2&doc=GetTRDOC.pdf>.

³ Hansman S., Hunt R., *A taxonomy of network and computer attacks*, în *Computers & Security*, (iun) 2004, p. 4, disponibil on-line la <http://ce.sharif.edu/courses/83-84/1/ce534/resorces/root/Papers/attacks>; Steichen P., *Advanced Security Methodologies – Computer and Network attacks*, pp. 15-16, disponibil on-line la http://pst.libre.eu/m2ssic-metz/02_attacks.pdf.

⁴ *Ibidem*.

⁵ Lough D. L., *A taxonomy ...*, *op. cit.*, p. 50.

Revenind la taxonomia dezvoltată, și la procesul care conduce această taxonomie, trebuie precizat că, față de taxonomia inițială (Howard, 1997), aceasta este structurată în 7 categorii (față de 5 categorii) și fiecare categorie este mai bine structurată și dezvoltată.

În prezentarea și explicarea taxonomiei dezvoltate, autorii identifică trei grupuri generale:

- **eveniment** – „o acțiune îndreptată către o țintă, intenționându-se a avea drept rezultat o schimbare a statusului țintei respective”¹ –, care include categoriile „acțiuni” și „ținte”, și este inclus grupul general „atac(uri)”;

- **atac(uri)** – „o serie de măsuri luate de un atacator pentru a obține un rezultat neautorizat”² –, care include, alături de grupul general „eveniment” și categoriile „unelte”, „vulnerabilitate” și „rezultate neautorizate” și este inclus în grupul general „incident”;

- **incident** – „un grup de atacuri care se pot distinge de alte atacuri datorită deosebirii atacatorilor, atacurilor, obiectivelor, localizării și sincronizării”³ – care include alături de grupul general „atac(uri)” și categoriile „atacatori” și „obiective”.

Alături de aceste grupuri generale identifică alți termeni mai generali care pot fi necesari pentru a putea descrie complet un incident⁴:

- locația (numele, numărul, cele care au raportat);
- data (raportării, începerii, încheierii);
- numărul incidentului;
- acțiunile corective.

Categoriile și subcategoriile incluse în taxonomia dezvoltată sunt următoarele:

a) **atacatorul** – „un individ care încearcă unul sau mai multe atacuri pentru a atinge un obiectiv” –; din această categorie fac parte:

- **hackeri** – „atacatori care atacă calculatorul pentru provocare, statut sau emoția obținerii accesului”;

- **spioni** – „atacatori care atacă calculatoarele pentru informații care să fie folosite pentru avantaje politice”;

- **teroriști** – „atacatori care atacă calculatoarele pentru a provoca teamă pentru avantaje politice”;

- **invadatori corporativi** – „angajați (atacatori) care atacă calculatoarele concurenților pentru câștig financiar”;

¹ Howard J. D., Longstaff T.A., *A Common Language ...*, op. cit., p. 7.

² *Ibidem*, p. 12.

³ *Ibidem*, p. 15.

⁴ *Ibidem*, pp. 17-18.

- **criminali profesioniști** - „atacatori care atacă calculatoarele pentru câștig financiar”;

- **vandali** - „atacatori care atacă calculatoarele pentru a provoca daune”.

b) **instrumentul** - „mijloc de exploatare a vulnerabilității unui calculator sau rețele”; din această categorie fac parte:

- **atac fizic** - „mijloc de a fura fizic sau a strica calculatorul, rețeaua, componentele sale sau sistemele de suport ale sale (cum ar fi aerul condiționat, energia electrică etc.)”;

- **schimb de informații** - „un mijloc de a obține informații de la alți „atacatori” (cum ar fi buletine electronice), sau de la persoane care au fost atacate (așa numita inginerie socială)”;

- **comandă a utilizatorului** - „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin intermediul introducerii de date direct de utilizator în interfața procesului. Un exemplu este introducerea comenzilor Unix prin intermediul unei conexiuni telnet sau de la un port SMTP”;

- **script sau program** - „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin executarea unui fișier de comenzi (script) sau a unui program în interfața procesului. Exemple sunt o sesiune Shell script pentru a exploata o eroare a programului, un program de conectare tip cal troian sau un program de spargere a parolei”;

- **agent autonom** - „un mijloc de exploatare a unei vulnerabilități prin utilizarea unui program sau a unui fragment dintr-un program care operează independent de utilizator. Exemple sunt virusii și viermii”;

- **kit de instrumente** - „un pachet de programe care conține scripturi, programe sau agenții autonome care exploatează vulnerabilitățile. Un exemplu este larg răspânditul kit de instrumente numit kit de acces la rădăcină”;

- **instrument distribuit** - „un instrument care poate fi distribuit la mai multe sisteme tip gazdă care pot fi apoi coordonate pentru a efectua în mod anonim un atac „după un anumit timp simultan asupra unor sisteme tip gazdă”;

- **interceptor de date** - „un mijloc de monitorizare a radiațiilor electromagnetice provenite de la un calculator sau rețea folosind un dispozitiv extern”.

c) **vulnerabilitate** - „un punct slab într-un sistem care să permită o acțiune neautorizată” -; din această categorie fac parte:

- **vulnerabilitate de proiectare** - „o vulnerabilitate în proiectarea sau specificațiile echipamentului sau programului care chiar și după o implementare perfectă va avea ca rezultat o vulnerabilitate”;

- **vulnerabilitate de implementare** - „o vulnerabilitate care rezultă dintr-o eroare în implementarea programului sau echipamentului care au fost proiectate corespunzător” -;

- **vulnerabilitate de configurare** - „o vulnerabilitate care rezultă dintr-o eroare în configurarea unui sistem, cum ar fi să ai un cont cu parole implicite, să ai permisiune de scriere... pentru fișiere noi sau să ai active servicii vulnerabile”.

d) **acțiune** - „o măsură luată de către un utilizator sau proces în vederea obținerii unui rezultat”; din această categorie fac parte:

- **sondare** - „accesarea unei ținte în vederea determinării caracteristicilor sale”;

- **scanare** - „accesarea secvențială a unui set de ținte în scopul de a identifica care țintă are o caracteristică specifică” -;

- **inundare** - „accesarea repetată a unei ținte în scopul de a supraîncărca capacitatea țintei” -;

- **autentificare** - „prezentarea identității cuiva unui proces și, dacă este necesar, verificarea acelei identități în vederea accesării unei ținte” -;

- **ocolire** - „evitarea unui proces prin utilizarea unei metode alternative de accesare a țintei” -;

- **păcălire** - „deghizare prin „asumarea apariției unei alte entități în rețea”;

- **citire** - „obținerea conținutului datelor din dispozitivele de stocare sau alte medii de date” -;

- **copiere** - „reproducerea unei ținte lăsând neschimbată ținta originală”;

- **furt** - „luarea în posesie a unei ținte fără a lăsa o copie în locația originală”;

- **modificare** - „schimbarea conținutului sau caracteristicilor unei ținte”;

- **ștergere** - „îndepărtarea unei ținte sau transformarea în irecuperabilă”.

e) **țintă** - „o entitate logică sau fizică a unui calculator sau rețele”:

- **cont** - „un domeniu pentru accesul utilizatorului pe un calculator sau rețea care este controlat ținându-se seama de o înregistrare de informații care conține numele contului utilizatorului, parola și restricții de utilizare”;

- **proces** - „un program în executare, constând în programul executabil, datele și stiva programului, controlul programului, indicatorul de stivă SP și alți regiștrii și toate celelalte informații necesare pentru executarea unui program”;

- **dată** - „reprezentarea de date, concepte sau instrucțiuni într-o manieră adecvată pentru comunicare, interpretare sau prelucrare de către om sau prin mijloace automate. Datele pot fi sub forma fișierelor, în memoria volatilă sau permanentă a calculatorului sau într-un dispozitiv de stocare, sau într-o formă de date în tranzit printr-un mediu de transmitere”;

- **componentă** - „una dintre părțile din care este făcut calculatorul sau rețeaua;

- **calculator** - „un dispozitiv care este alcătuit din unul sau mai multe componente asociate, inclusiv unitatea de procesare și unitățile periferice, care este controlată de programe stocate intern și care poate efectua calcule substanțiale,

incluzând numeroase operațiuni matematice sau operațiuni logice, fără intervenție umană în timpul execuției”;

- **rețea** – „un grup de calculatoare gazdă interconectate și interdependente, elemente de comutare și ramificații interconectate”;

- **inter-rețele** – „o rețea de rețele”.

f) **rezultat neautorizat** – „o consecință neautorizată a unui eveniment”; din această categorie fac parte:

- **acces crescut** – „o creștere neautorizată în domeniul de acces de pe un calculator sau rețea”;

- **divulgare de informații** – „diseminarea de informații către orice persoană care nu este autorizată să acceseze acele informații”;

- **falsificare de informații** – „modificarea neautorizată a datelor de pe un calculator sau rețea”;

- **refuzare a serviciului** – „deteriorarea sau blocarea intenționată a resurselor calculatorului sau rețelei”;

- **furt de resurse** – „utilizarea neautorizată a resurselor calculatorului sau rețelei”;

g) **obiective** – „scopul sau obiectivul final al unui incident”; din această categorie fac parte:

- **provocare, status, emoție;**

- **câștiguri politice;**

- **câștiguri financiare;**

- **pagubă.**

Taxonomia completă este prezentată de autori sub formă grafică¹ fiind evidențiată relația dintre evenimente, de la atacuri la incidente, și sugerează că prevenirea îndeplinirii obiectivelor atacatorilor ar putea fi realizată prin asigurarea faptului că un atacator nu ar reuși parcurgerea celor șapte pași descriși mai sus.

§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare²

Taxonomia dezvoltată de acest autor, a fost creată special pentru testarea și evaluarea sistemelor de detectare a intruziunilor (IDS).

¹ *Ibidem*, p. 16.

² Weber D.J., *A Taxonomy of Computer Intrusions*, lucrare de dizertație susținută la Massachusetts Institute of Technology, (iun.) 1998, disponibil on-line la <http://dspace.mit.edu/bitstream/handle/1721.1/9861/41473759.pdf>.

Autorul consideră¹ „taxonomia necesită un mod de descriere a nivelurilor privilegiului, un mod de descriere a tranzițiilor și un mod de clasificare a acțiunilor”. Astfel:

(1) **niveluri ale privilegiului utilizatorului:**

- a) **fără acces (O)**, când nu are practic acces la un sistem;
- b) **rețea la distanță (R)**, când are un minim acces de rețea la un sistem prin intermediul altor rețele;
- c) **rețea locală (L)**, când are abilitatea să citească și să scrie în rețeaua locală ceea ce dispozitivul țintă folosește;
- d) **acces modem (M)**, când are abilitatea să se conecteze direct la un calculator țintă;
- e) **acces utilizator (U)**, când are abilitatea să ruleze comenzi normale de utilizator;
- f) **acces la rădăcină/status de administrator (S)**, când are acces total la sistem.

(2) **acțiuni:**

- a) **sondare**, în situația în care sunt colectate datele despre sistem:
 - **sondare (Utilizator)**, când privesc utilizatorul dispozitivului;
 - **sondare (Serviciu)**, când privesc serviciile dispozitivului;
 - **sondare (Dispozitiv)**, când privesc dispozitivele în rețea.
- b) **refuz al serviciului**, în situația în care este împiedicat accesul legitim la sistem (include deteriorarea serviciului):
 - **Refuz (Temporar)**, când refuzul este temporar, cu recuperare automată;
 - **Refuz (Administrativ)**, când refuzul necesită acțiunea administratorului pentru recuperare;
 - **Refuz (Permanent)**, când refuzul este permanent.
- c) **interceptare/citire a datelor**, în situația în care sunt interceptate/citite datele:
 - **interceptare (Fișiere)**, când sunt vizate fișierele unui sistem;
 - **interceptare (Rețea)**, când este vizat traficul de rețea.
- d) **alterare/creare a datelor**, în situația în care sunt alterate/create datele:
 - **Alterare (Date)**, când vizează alterarea datelor stocate;
 - **Alterare (Urmărire, intruziune)**, când vizează înlăturarea urmelor intruziunii.
- e) **utilizare a sistemului de către atacatori**, în situația în care sistemul țintă este utilizat de atacator:
 - **Utilizare (Recreațională)**, când vizează utilizarea sistemului pentru distracție;

¹ *Ibidem*, p. 40.