

# Obsah

<b>1. Vznik kyberprostoru .....</b>	<b>15</b>
<b>1.1 Chápání kyberprostoru .....</b>	<b>17</b>
<b>2. Pět problémů kybernality .....</b>	<b>19</b>
<b>2.1 Problém první – hrozby .....</b>	<b>20</b>
2.1.1 Taxonomie hrozby .....	21
2.1.2 Charakter hrozby a její cíl .....	24
<b>2.2 Problém druhý – legislativa .....</b>	<b>25</b>
<b>2.3 Problém třetí – policie a justice .....</b>	<b>26</b>
2.3.1 Praxe v České republice .....	28
<b>2.4 Problém čtvrtý – společnost .....</b>	<b>29</b>
<b>2.5 Problém pátý – chápání bezpečnosti .....</b>	<b>30</b>
<b>3. Kyberprostor a společnost .....</b>	<b>33</b>
<b>3.1 Populace kyberprostoru .....</b>	<b>35</b>
<b>3.2 Netholismus a netománie .....</b>	<b>36</b>
<b>3.3 Chat a chataři .....</b>	<b>39</b>
3.3.1 Rozvraceči .....	42
<b>3.4 Pařani .....</b>	<b>43</b>
<b>4. Hackeri a crackeri .....</b>	<b>47</b>
<b>4.1 Historie hackingu .....</b>	<b>47</b>
<b>4.2 Definice hackera .....</b>	<b>51</b>
<b>4.3 Hackeri v kyberprostoru .....</b>	<b>52</b>
4.3.1 Morální hodnoty hackerské komunity .....	52
4.3.2 Hackerský jazyk a humor .....	53
4.3.3 Typy hackerů .....	54
4.3.4 Osobnosti hackingu .....	56

<b>4.4 Hackerské programové nástroje .....</b>	<b>59</b>
4.4.1 Vývoj hackerských nástrojů .....	59
4.4.2 Prolamovače hesel .....	62
4.4.3 Backdoors .....	63
4.4.4 Skenery .....	64
4.4.5 Sniffery .....	64
4.4.6 Rootkity .....	65
4.4.7 Nástroje DoS .....	66
4.4.8 Trojské koně .....	67
4.4.9 Nástroje průzkumu sítě .....	67
4.4.10 Debugery .....	67
<b>4.5 Warez .....</b>	<b>68</b>
4.5.1 Warez a jeho organizace .....	69
4.5.2 Příslušníci warez scény a jejich motivace .....	71
4.5.3 Prostředky šíření pirátských dat .....	72
4.5.4 Válka s warez scénou – případ nikdy nekončícího souboje .....	73

## **5. Kyberprostor a právo .....** **75**

<b>5.1 Krátký kurs trestního práva pro informatiky .....</b>	<b>77</b>
5.1.1 Zásady trestního práva .....	77
5.1.2 Trestní právo a související obory .....	79
5.1.3 Výklad trestních zákonů .....	80
5.1.4 Působnost trestních zákonů .....	82
5.1.5 Trestný čin .....	83
5.1.6 Pachatel .....	84
5.1.7 Trestní právo procesní .....	86
<b>5.2 Legislativní zázemí postihu kybernetické kriminality .....</b>	<b>88</b>
5.2.1 Česká legislativa .....	89
5.2.2 Mezinárodní legislativní aktivity .....	90
<b>5.3 Jak definovat kybernetickou kriminalitu .....</b>	<b>91</b>
5.3.1 Klasifikace podle mezinárodní dohody o kyberzločinu .....	91
5.3.2 Klasifikace podle eEurope+ .....	92
5.3.3 Klasifikace podle dopadu konkrétního skutku .....	92
5.3.4 Klasifikace kybernetičtosti z hlediska skutkových podstat .....	93
<b>5.4 Vztahy autorské a vlastnické v kybernetické oblasti .....</b>	<b>95</b>
5.4.1 Autorské právo a programová díla .....	96

<b>5.5 Program, data a databáze.....</b>	<b>99</b>
5.5.1 Definice programu .....	99
5.5.2 Data a databáze .....	100
5.5.3 Porušování autorských práva k programu .....	100
<b>5.6 Nové typy protiprávního jednání .....</b>	<b>102</b>
5.6.1 Hacking .....	102
5.6.2 Kybernetické výpalné .....	102
5.6.3 Šíření materiálů se závadným obsahem .....	103
5.6.4 Zneužití internetových stránek .....	103
5.6.5 Spamming .....	104
5.6.6 Warez .....	105
5.6.7 Cracking .....	106
5.6.8 Sniffing .....	106
5.6.9 Cybersquatting .....	107

## **6. Nelegální aktivity v kyberprostoru..... 109**

<b>6.1 Metody pachatelů kybernality.....</b>	<b>111</b>
<b>6.2 Insideri a nespokojení zaměstnanci .....</b>	<b>114</b>
6.2.1 Možnosti jednotlivých profesí .....	115
6.2.2 Co říkají statistiky a průzkumy .....	117
6.2.3 Kategorizace nelegálních aktivit zaměstnanců .....	120
<b>6.3 Vliv lidského faktoru na únik informací.....</b>	<b>123</b>
6.3.1 Nerozpoznání možné hrozby .....	124
6.3.2 Nedokonalá normativní báze .....	125
6.3.3 Problém bezpečnostní kultury .....	125
6.3.4 Obchodní partneři a zaměstnanci .....	126
6.3.5 Možná obrana proti úniku informací .....	127
<b>6.4 Terorismus a jeho projekce do kyberprostoru .....</b>	<b>128</b>
<b>6.5 Kyberterorismus .....</b>	<b>130</b>
6.5.1 Taxonomie útočníků podle geopolitického hlediska .....	132
6.5.2 Aktivity teroristů vůči informačním technologiím .....	134
6.5.3 Komunikační kanály teroristických skupin .....	136
6.5.4 Ideologické zneužívání kyberprostoru .....	137
<b>6.6 Teroristické aktivity související s IT .....</b>	<b>144</b>
6.6.1 Mediální terorismus .....	144
6.6.2 Procesní terorismus .....	146
6.6.3 IT governance .....	147
6.6.4 Trendy kyberterorismu .....	148

<b>7. Kybernetické války a infoware .....</b>	<b>151</b>
<b>7.1 Metody informačního boje a jejich účinky .....</b>	<b>152</b>
<b>7.2 Informační válka .....</b>	<b>153</b>
<b>7.3 Command-and-Control Warfare .....</b>	<b>155</b>
<b>7.4 Zpravodajský warfare .....</b>	<b>156</b>
7.4.1 Útočné prostředky infoware .....	156
7.4.2 Obranné prostředky infoware .....	156
<b>7.5 Elektronický warfare .....</b>	<b>157</b>
7.5.1 Radioelektronický warfare .....	157
7.5.2 Kryptografický warfare .....	157
<b>7.6 Psychologický warfare.....</b>	<b>158</b>
<b>7.7 Hacker<sup>10</sup> warfare.....</b>	<b>159</b>
<b>7.8 Ekonomický informační warfare.....</b>	<b>161</b>
7.8.1 Informační blokáda .....	161
7.8.2 Informační imperialismus .....	162
<b>7.9 Kybernetický warfare.....</b>	<b>162</b>
<b>7.10 Infoware versus konvenční ozbrojené složky .....</b>	<b>163</b>
<b>7.11 Budoucí perspektivy vývoje infoware .....</b>	<b>163</b>
<b>7.12 Příklady informačních střetů.....</b>	<b>164</b>
7.12.1 Konflikt v Kosovu .....	164
7.12.2 Americko-čínský konflikt v roce 2001 .....	166
7.12.3 Další významné střety v kyberprostoru .....	167
<b>8. Průmyslová špionáž .....</b>	<b>169</b>
<b>8.1 Známá fakta .....</b>	<b>170</b>
<b>8.2 Únik informací klasickou formou .....</b>	<b>170</b>
8.2.1 Technologické kanály .....	171
8.2.2 Sběr informací v sítích .....	174
<b>9. Globální odposlech .....</b>	<b>179</b>
<b>9.1 Historie globálního odposlechu .....</b>	<b>180</b>
9.1.1 Aliance UK/USA .....	181
9.1.2 Úloha NSA v digitálním zpravodajství – Echelon .....	183
9.1.3 Ekonomické využití Echelonu.....	185

<b>9.2 Technologie Echelonu .....</b>	<b>185</b>
9.2.1 Vyhledávání zájmových informací .....	188
9.2.3 Odposlech internetu .....	191
<b>9.3 FAPSI a SOUD .....</b>	<b>192</b>
<b>10. Sociální inženýrství .....</b>	<b>195</b>
<b>10.1 Metody sociologického útoku .....</b>	<b>196</b>
10.1.1 Volné zdroje .....	197
10.1.2 Budování důvěry .....	199
<b>10.2 Prostředky a cíle sociotechnického útoku .....</b>	<b>200</b>
10.2.1 Telefonní útoky .....	200
10.2.2 Metody přesvědčování obětí .....	201
10.2.3 Útoky nástroji internetové komunikace .....	203
<b>10.3 Obrana proti sociálnímu inženýrství .....</b>	<b>206</b>
<b>11. Informatické útoky .....</b>	<b>209</b>
<b>11.1 Taxonomie informatického útoku .....</b>	<b>209</b>
<b>11.2 Zobecnění útoků v distribuovaném informačním systému .....</b>	<b>212</b>
11.2.1 Analýza síťového toku .....	215
11.2.2 Substitutece důvěryhodného objektu .....	216
11.2.3 Podvržení falešného objektu .....	218
11.2.4 Útok potlačením služby (DoS) .....	223
<b>11.3 Protokoly a metody pro mapování prostředí – internetu .....</b>	<b>226</b>
11.3.1 Mapování s využitím protokolu ICMP .....	226
11.3.2 Použití protokolu UDP .....	227
11.3.3 Použití protokolu TCP .....	227
11.3.4 Problémy spojené s trasovacími metodami .....	228
<b>11.4 Odhalování adresové struktury internetu .....</b>	<b>229</b>
11.4.1 Metoda využívající broadcast ping (všesměrový ping) .....	229
11.4.2 Odvozování masky na základě skupiny IP adres. ....	230
11.4.3 Hádání platných adres .....	231
11.4.4 Inverzní mapování .....	232
<b>11.5 Generování topologie sítě .....</b>	<b>233</b>
11.5.1 Implementace s protokolem SNMP .....	233
11.5.2 Použití DNS a broadcast ping .....	234
11.5.3 Použití trasování .....	235

<b>11.6 Identifikace zdrojů v internetu .....</b>	<b>235</b>
11.6.1 Skenování portů .....	236
<b>11.7 Techniky identifikace operačního systému .....</b>	<b>236</b>
11.7.1 Metoda „banner grabbing“ .....	238
11.7.2 Skenování otevřených portů .....	239
11.7.3 Dotazování IP zásobníku .....	239
11.7.4 Pasivní detekce OS .....	243
11.7.5 Obecné shrnutí .....	247
<b>12. Vyšetřování kybernetického deliktu .....</b>	<b>251</b>
<b>12.1 Vyšetřovací rámec .....</b>	<b>252</b>
12.1.1 Prevence .....	252
12.1.2 Detekce průniku .....	253
<b>12.2 Metodika vyšetřování .....</b>	<b>254</b>
12.2.1 Trasování k iniciátorovi průniku .....	256
12.2.2 Analýza cesty .....	257
12.2.3 Informační zdroje na internetu .....	259
<b>12.3 Role orgánů činných v trestním řízení .....</b>	<b>260</b>
<b>12.4 Role privátních vyšetřovatelů, znalců a konzultantů .....</b>	<b>260</b>
<b>12.5 Vyšetřovací tým .....</b>	<b>261</b>
12.5.1 Struktura vyšetřovacího týmu .....	261
12.5.2 Ustavení vyšetřovacího týmu .....	262
12.5.3 Zodpovědnosti členů týmu .....	263
12.5.4 Klasifikace incidentu .....	266
<b>13. Slovník pojmů .....</b>	<b>269</b>
<b>14. Význam některých zkratek .....</b>	<b>275</b>
<b>Rejstřík .....</b>	<b>279</b>