

Obsah

1. Vznik kyberprostoru	15
1.1 Chápání kyberprostoru.....	17
2. Pět problémů kybernalitý	19
2.1 Problém první – hrozby	20
2.1.1 Taxonomie hrozby	21
2.1.2 Charakter hrozby a její cíl	24
2.2 Problém druhý – legislativa	25
2.3 Problém třetí – policie a justice	26
2.3.1 Praxe v České republice	28
2.4 Problém čtvrtý – společnost.....	29
2.5 Problém pátý – chápání bezpečnosti	30
3. Kyberprostor a společnost	33
3.1 Populace kyberprostoru	35
3.2 Netholismus a netománie.....	36
3.3 Chat a chataři	39
3.3.1 Rozvraceči.....	42
3.4 Pařani.....	43
4. Hackeri a crackeři	47
4.1 Historie hackingu.....	47
4.2 Definice hackera	51
4.3 Hackeri v kyberprostoru	52
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

4.4 Hackerské programové nástroje	59
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 Debuggery	67
4.5 Warez	68
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
5.1 Krátký kurs trestního práva pro informatiky	77
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
5.2 Legislativní zázemí postihu kybernetické kriminality	88
5.2.1 Česká legislativa	89
5.2.2 Mezinárodní legislativní aktivity	90
5.3 Jak definovat kybernetickou kriminalitu	91
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
5.4 Vztahy autorské a vlastnické v kybernetické oblasti	95
5.4.1 Autorské právo a programová díla	96

5.5 Program, data a databáze.....	99
5.5.1 Definice programu	99
5.5.2 Data a databáze	100
5.5.3 Porušování autorských práva k programu	100
5.6 Nové typy protiprávního jednání	102
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
6.1 Metody pachatelů kybernalit.....	111
6.2 Insideri a nespokojení zaměstnanci	114
6.2.1 Možnosti jednotlivých profesí	115
6.2.2 Co říkají statistiky a průzkumy	117
6.2.3 Kategorizace nelegálních aktivit zaměstnanců	120
6.3 Vliv lidského faktoru na únik informací.....	123
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
6.4 Terorismus a jeho projekce do kyberprostoru	128
6.5 Kyberterorismus	130
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
6.6 Teroristické aktivity související s IT	144
6.6.1 Mediální terorismus	144
6.6.2 Procesní terorismus	146
6.6.3 IT governance	147
6.6.4 Trendy kyberterorismu	148

7. Kybernetické války a infoware	151
7.1 Metody informačního boje a jejich účinky	152
7.2 Informační válka	153
7.3 Command-and-Control Warfare	155
7.4 Zpravodajský warfare	156
7.4.1 Útočné prostředky infoware	156
7.4.2 Obranné prostředky infoware	156
7.5 Elektronický warfare	157
7.5.1 Radioelektronický warfare	157
7.5.2 Kryptografický warfare	157
7.6 Psychologický warfare.....	158
7.7 Hacker¹⁰ warfare.....	159
7.8 Ekonomický informační warfare.....	161
7.8.1 Informační blokáda	161
7.8.2 Informační imperialismus	162
7.9 Kybernetický warfare.....	162
7.10 Infoware versus konvenční ozbrojené složky	163
7.11 Budoucí perspektivy vývoje infoware	163
7.12 Příklady informačních střetů.....	164
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
 8. Průmyslová špionáž	 169
8.1 Známá fakta	170
8.2 Únik informací klasickou formou	170
8.2.1 Technologické kanály	171
8.2.2 Sběr informací v sítích	174
 9. Globální odposlech	 179
9.1 Historie globálního odposlechu	180
9.1.1 Aliance UK/USA	181
9.1.2 Úloha NSA v digitálním zpravodajství – Echelon	183
9.1.3 Ekonomické využití Echelonu.....	185

9.2 Technologie Echelonu	185
9.2.1 Vyhledávání zájmových informací	188
9.2.3 Odposlech internetu	191
9.3 FAPSI o SOUD	192
10. Sociální inženýrství	195
10.1 Metody sociologického útoku	196
10.1.1 Volné zdroje	197
10.1.2 Budování důvěry	199
10.2 Prostředky a cíle sociotechnického útoku	200
10.2.1 Telefonní útoky	200
10.2.2 Metody přesvědčování obětí	201
10.2.3 Útoky nástroji internetové komunikace	203
10.3 Obrana proti sociálnímu inženýrství	206
11. Informatické útoky	209
11.1 Taxonomie informatického útoku	209
11.2 Zobecnění útoků v distribuovaném informačním systému	212
11.2.1 Analýza síťového toku	215
11.2.2 Substituce důvěryhodného objektu	216
11.2.3 Podvržení falešného objektu	218
11.2.4 Útok potlačením služby (DoS)	223
11.3 Protokoly a metody pro mapování prostředí – internetu	226
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
11.4 Odhalování adresové struktury internetu	229
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
11.5 Generování topologie sítě	233
11.5.1 Implementace s protokolem SNMP	233
11.5.2 Použití DNS a broadcast ping	234
11.5.3 Použití trasování	235

11.6 Identifikace zdrojů v internetu	235
11.6.1 Skenování portů	236
11.7 Techniky identifikace operačního systému	236
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
12. Vyšetřování kybernetického deliktu	251
12.1 Vyšetřovací rámec	252
12.1.1 Prevence	252
12.1.2 Detekce průniku	253
12.2 Metodika vyšetřování	254
12.2.1 Trasování k iniciátorovi průniku	256
12.2.2 Analýza cesty	257
12.2.3 Informační zdroje na internetu	259
12.3 Role orgánů činných v trestním řízení	260
12.4 Role privátních vyšetřovatelů, znalců a konzultantů	260
12.5 Vyšetřovací tým	261
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
13. Slovník pojmů	269
14. Význam některých zkratek	275
Rejstřík	279