**Předmluva vydavatele** 7

**Předmluva autora** 11

**Seznam zkratek** 27

**1 Pojem kybernetické trestné činnosti a pojmy související** 31
1.1 Kybernetická trestná činnost (Cybercrime) 31
1.2 Pojmy související s kybernetickou trestnou činností 42
1.2.1 Kyberprostor (Cyberspace) 42
1.2.2 Kybernetický útok (Cyber attack) 54
1.2.3 Počítač (Počítačový systém) 57
1.2.3.1 Hardware 59
1.2.3.2 Software 62
1.2.3.3 Data a informace 65
1.3 Počítačové sítě a jejich fungování 67
1.3.1 Počítačová síť (Computer network) 67
1.3.2 Internet Protocol a IP adresa 74
1.3.3 MAC Adresa 77
1.4 ISP (Internet Service Provider) 78

**2 Působnost práva v kyberprostoru** 85
2.1 Právní prostředí Internetu obecně 91
2.2 Prostředky trestního práva 93
2.2.1 Prostředky trestního práva hmotného 93
2.2.2 Prostředky trestního práva procesního 96
2.3 Prostředky správního práva 97
2.4 Prostředky občanského práva 99
2.4.1 Ochrana soukromí 99
2.4.2 Věci a virtuální majetek 101
2.4.3 Právní jednání 107
2.4.4 Licence 107
2.4.5 Náhrada škody 108
2.5 Odpovědnost poskytovatele služeb informační společnosti 109
2.5.1 Poskytovatelé služeb spočívajících v přenosu informací poskytnutých uživatelem (Mere Conduit či Access Provider) 114
2.5.1.1 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZSIS 116
2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK 116

2.5.2 Poskytovatelé služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. caching) 124
2.5.3 Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting) 125
2.6 Možnosti právní odpovědnosti uživatele za jednání v kyberprostoru 126

**3 Anonymita uživatele 133**
3.1 Digitální stopa 134
3.1.1 Digitální stopa neovlivnitelná 135
3.1.2 Digitální stopa ovlivnitelná 144
3.2 Smluvní podmínky (EULA) 145
3.3 Sociální sítě 151
3.4 Projekty testující zranitelnosti uživatelů sociálních sítí 156
3.4.1 Dennis a Terezka 158
3.4.2 Petr Dvořák 162
3.4.3 Adam Novák 169
3.5 Doporučení pro uživatele sociálních sítí 172
3.6 Právo být zapomenut 174

**4 Projevy kyberkriminality 181**
4.1 Sociální inženýrství (Sociotechnika) 186
4.2 Botnet 193
4.3 Malware 204
4.4 Ransomware 221
4.5 Spam 231
4.5.1 Scam 419 236
4.5.2 Hoax 240
4.5.3 Podvodné nabídky 240
4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing 246
4.6.1 Phishing 246
4.6.1.1 Dluh/Banka/Exekuce 250
4.6.1.2 Česká pošta 255
4.6.1.3 Vánoce a dárky 260
4.6.1.4 Seznam.cz – One Time Password 261
4.6.2 Pharming 263
4.6.3 Spear Phishing 264
4.6.4 Vishing 265
4.6.5 Smishing 266
4.7 Podvodné webové stránky (firmy) 266
4.8 Hacking 269
4.9 Cracking 276

4.10 Internetové (počítačové) pirátství 277
4.10.1 Právo duševního vlastnictví 277
4.10.2 Legislativní rámec 278
4.10.3 Autorské právo 280
4.10.4 Vlastní útoky 286
4.10.5 Možná řešení 290
4.11 Sniffing 294
4.12 DoS, DDoS, DRDoS útoky 295
4.13 Šíření závadového obsahu 305
4.14 Kybernetické útoky na sociálních sítích 309
4.14.1 Kyberšikana 309
4.14.2 Kybergrooming 312
4.14.3 Sexting 314
4.14.4 Kyberstalking 317
4.15 Identity theft 318
4.16 APT (Advanced Persistent Threat) 320
4.17 Kyberterorismus 323
4.18 Další útoky 326
4.18.1 Cybersquatting, typosquatting 326
4.18.2 Útoky na VoIP 327
4.18.3 Kybernetické výpalné (Racketeering) 327

**5 Trestněprávní ochrana před kyberkriminalitou 331**
5.1 Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU 332
5.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě 332
5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě 334
5.1.3 Dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti 335
5.1.4 Právní normy ČR 338
5.2 Hmotněprávní aspekty kybernetické trestné činnosti 338
5.2.1 Kybernetické trestné činy ve zvláštní části trestního zákoníku 338
5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku 344
5.2.2.1 Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů 344
5.2.2.1.1 Neoprávněný přístup (čl. 2) 344
5.2.2.1.2 Neoprávněné zachycení informací (čl. 3) 347
5.2.2.1.3 Zásah do dat (čl. 4) 352
5.2.2.1.4 Zásah do systému (čl. 5) 355
5.2.2.1.5 Zneužití zařízení (čl. 6) 357
5.2.2.2 Trestné činy ve vztahu k počítači 361

5.2.2.2.1 Padělání související s počítači (čl. 7) 361
5.2.2.2.2 Podvod související s počítači (čl. 8) 362
5.2.2.3 Trestné činy se vztahem k obsahu počítače 364
5.2.2.3.1 Trestné činy související s dětskou pornografií (čl. 9) 365
5.2.2.3.2 Šíření rasismu a xenofobie 371
5.2.2.4 Trestné činy se vztahem k autorským nebo obdobným právům (čl. 10) 372
5.2.2.5 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZK) 376
5.2.2.6 Ostatní ustanovení trestního zákoníku mající vztah ke kybernetické kriminalitě 378
5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru 379
5.3.1 Charakteristika sdružení CZ.NIC a vymezení zkoumaných otázek 381
5.3.1.1 Charakteristika sdružení CZ.NIC, z.s.p.o. 381
5.3.1.2 Vlastní předmět zkoumání 383
5.3.1.3 Výklad použitý při analýze zkoumaných otázek 384
5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC 385
5.3.2.1 Zisk a analýza volně dostupných informací (pasivní analýza) 387
5.3.2.2 Skenování zranitelnosti (aktivní analýza) 389
5.3.2.3 Aktivní testování zabezpečení ICT (Přístup k počítačovému systému a nosiči informací) 391
5.3.3 Právní normy, které mohou být analýzami sdružení CZ.NIC dále dotčeny 396
5.3.4 Shrnutí studie 397

**6 Trestněprocesní a kriminalistické aspekty odhalování, prověřování a vyšetřování kyberkriminality 401**
6.1 Kriminalistická metodika vyšetřování kybernetické kriminality 401
6.1.1 Digitální stopa 402
6.1.2 Kriminální situace 406
6.1.3 Zvláštnosti předmětu vyšetřování 406
6.1.4 Zvláštnosti podnětů k vyšetřování 407
6.1.5 Zvláštnosti vyšetřovacích verzí a organizace vyšetřování 408
6.1.6 Zvláštnosti následných úkonů 409
6.2 Trestněprocesní postup při odhalování, prověřování a vyšetřování kyberkriminality 410
6.2.1 Specifika přijetí trestního oznámení a prověřování 410
6.2.1.1 Určení místní příslušnosti OČTŘ 413
6.2.1.2 Součinnost státních orgánů, fyzických a právnických osob 414
6.3 Specifika dokazování kyberkriminality 417
6.3.1 Věcné a listinné důkazy 417
6.3.1.1 Věcné důkazy 417
6.3.1.2 Listinné důkazy 418
6.3.1.3 Digitální důkazy 419

6.4 Specifika zajišťovacích úkonů 419
6.4.1 Vydání a odnětí věci 420
6.4.2 Zajištění nehmotné věci a zajištění peněžních prostředků na účtu u banky 423
6.4.3 Domovní prohlídka 424
6.4.4 Prohlídka jiných prostor a pozemků 429
6.4.5 Odposlech a záznam telekomunikačního provozu 431
6.4.5.1 Telekomunikační provoz 431
6.4.5.2 Odposlech a záznam telekomunikačního provozu 437
6.4.5.3 Zjištění údajů o telekomunikačním provozu 442
6.4.6 Operativně pátrací prostředky 446
6.4.6.1 Sledování osob a věcí 447
6.4.6.2 Použití agenta 449
6.5 Znalec 451

**7 Náměty de lege ferenda 459**
7.1 Trestní právo hmotné 459
7.1.1 Místní působnost trestního zákoníku 459
7.1.2 Trestněprávní ochrana před neoprávněným přístupem k počítačovému systému 460
7.1.3 Ochrana dětí před kybergroomingem 460
7.1.4 Trestněprávní ochrana před DoS a DDoS útoky 461
7.1.5 Botnet 461
7.1.6 Sankce a trestnost přípravy 462
7.1.7 Rozšíření oznamovací povinnosti 464
7.1.8 Doplnění kvalifikačních okolností 464
7.2 Trestní právo procesní 465
7.2.1 Urychlené uchování uložených počítačových dat 465
7.2.2 Příkaz k předložení, prohlídka a zajištění uložených počítačových dat 466
7.2.3 Digitální důkaz 469
7.2.4 Virtuální (krypto) měna 469

**Závěr 473**

**Seznam použitých pramenů a dalších zdrojů 479**

**Rejstřík 511**