

Obsah

O autorce	V
Předmluva.....	VII
Seznam použitých zkratk.....	XIII
Úvod.....	1
ČÁST PRVNÍ. Globální informační sítě, digitální revoluce a proměny společnosti.....	9
KAPITOLA I. Digitální revoluce a informační společnost.....	9
1. Digitální revoluce, globalizace a společenské změny.....	9
2. Základní pojmy – počítač, data, informace, kyberprostor a Internet.....	15
3. Rizikové faktory sítě Internet	20
3.1 Globální dosah.....	20
3.2 Decentralizovaná architektura a anonymita.....	20
3.3 Informační hodnota, snadná manipulace s daty a automatizace	21
3.4 Rychlý koloběh inovace.....	22
3.5 Konflikt mezi soukromou a veřejnou správou.....	23
4. Vliv globálních informačních sítí na pojetí informace.....	24
KAPITOLA II. Hodnoty informační společnosti.....	28
1. Svoboda projevu a svoboda šířit a přijímat informace (informační svoboda)	28
2. Informační sebeurčení.....	31
KAPITOLA III. Principy a východiska kybernetické bezpečnosti	35
1. K právním principům.....	36
2. Obecné principy správního práva	37
2.1 Principy dobré správy	39
2.2 Princip odpovědnosti veřejné správy.....	41
3. Principy práva kybernetické bezpečnosti	44
3.1 Technologická neutralita.....	44
3.2 Ochrana informačního sebeurčení člověka.....	46

3.3	Ochrana nedistributivních práv	48
3.4	Minimalizace státního donucení	51
3.5	Autonomie vůle regulovaných subjektů.....	52
3.6	Bdělost ve vztahu k ostatním státům a k mezinárodnímu společenství.....	53
KAPITOLA IV. Působení práva v kyberprostoru.....		56
1.	Legitimita práva v kyberprostoru	56
2.	Vymahatelnost právních norem v kyberprostoru	58
3.	Regulace kyberprostoru jinou než právní normou.....	59
4.	Suverenita, jurisdikce a kyberprostor	61
4.1	Suverenita státu	63
4.2	Jurisdikční principy	64
4.3	Jurisdikční konflikty.....	66
4.4	Tallinnský manuál.....	68
4.5	Rozhodnutí SDEU ve věci <i>Google vs. CNIL</i>	72
ČÁST DRUHÁ. Kyberprostor a úloha státu na zajištění informační bezpečnosti		75
KAPITOLA I. Kybernetická bezpečnost i kybernetická obrana jako úloha státu		75
1.	Kyberprostor a vázanost státní moci zákonem	75
2.	Bezpečnost	77
3.	Kybernetická bezpečnost	80
3.1	Definice	80
3.2	Akt EU o kybernetické bezpečnosti – nařízení 2019/881	83
3.3	Nařízení o Evropské síti a centru kompetencí pro kybernetickou bezpečnost – nařízení 2021/887	85
3.4	Národní strategie kybernetické bezpečnosti 2021–2025	87
3.5	Akční plán k Národní strategii kybernetické bezpečnosti 2021–2025	90
4.	Kybernetická obrana	92
4.1	Definice	92
4.2	Zákonná pravomoc Vojenského zpravodajství – detekce, vyhodnocení i reakce na kybernetické útoky a hrozby	93
4.3	Kontrola výkonu činnosti Vojenského zpravodajství v oblasti kybernetické obrany státu.....	97
KAPITOLA II. Pojmové znaky bezpečnosti informací a dat		100
1.	Důvěrnost informací a dat.....	101
2.	Integrita (celistvost) informací a dat.....	105
3.	Dostupnost informací a dat	106

KAPITOLA III. Narušení bezpečnosti informací, služeb a sítí ...	108
1. Kybernetická bezpečnostní událost a incident	108
2. Kybernetický útok	109
3. Příklady narušení důvěrnosti a celistvosti informací a dat.....	112
4. Narušení dostupnosti informací a dat	115
4.1 Příklady	115
4.2 Exkurz – <i>Stuxnet</i>	119
5. Přehled vybraných právních předpisů a norem.....	121
5.1 Úmluva o počítačové kriminalitě.....	121
5.2 Opatření pro budování důvěry v kyberprostoru.....	125
5.3 <i>Tallinn Manual 2.0</i>	128
5.4 Směrnice NIS.....	131
5.5 Směrnice NIS2.....	133
5.6 Zákon o kybernetické bezpečnosti a vyhláška o kybernetické bezpečnosti	141
5.7 Standardy a normy	144
 KAPITOLA IV. Kybernetické operace a mezinárodní odpovědnost státu	 146
1. Nestátní aktéři jako původci kybernetických operací	146
2. Státní aktéři jako původci kybernetických operací	150
3. Přičitatelnost (atribuce)	153
3.1 Přičitatelnost kybernetických operací státním orgánům.....	153
3.2 Přičitatelnost kybernetických operací nestátním aktérům	155
4. Okolnosti vylučující protiprávnost kybernetických operací	157
4.1 Přehled okolností vylučujících protiprávnost.....	157
4.2 Vybrané okolnosti vylučující protiprávnost: Protiopatření ...	159
4.3 Vybrané okolnosti vylučující protiprávnost: Krajní nouze ...	162
5. <i>Hack-back</i> , aktivní kyberobrana.....	165
6. Odpovědnost státu za mezinárodně protiprávní čin v kyberprostoru	169
 ČÁST TŘETÍ. Zákon o kybernetické bezpečnosti	 173
 KAPITOLA I. Nová právní úprava kybernetické bezpečnosti	 173
1. Okolnosti a důvody přijetí nové právní úpravy	173
2. Východiska právní úpravy, vztah ke směrnici NIS.....	175
3. Vývoj právní úpravy.....	177
 KAPITOLA II. Systém zajištění kybernetické bezpečnosti	 181
1. Bezpečnostní opatření (§ 4 a 5 KybBez).....	183
2. Opatření v užším slova smyslu (§ 11 KybBez)	189
2.1 Varování (§ 12 KybBez)	189
2.2 Reaktivní opatření (§ 13 a 15 KybBez)	200
2.3 Ochranné opatření (§ 14 a 15 KybBez).....	208

3. Nápravná opatření (§ 24 KybBez)	210
4. Rozhodnutí o uložení povinnosti předat data, provozní údaje a informace (§ 15a KybBez)	214
KAPITOLA III. <i>Computer Emergency Response Team</i> (CERT) ...	217
1. Národní CERT – příklad privatizace veřejné správy.....	218
2. Vládní CERT	225
KAPITOLA IV. Zvláštní kontrolní orgán Poslanecké sněmovny PČR.....	228
Závěr.....	233
1. Ke společenským proměnám, hodnotám a principům informační společnosti a k působení právních norem v kyberprostoru.....	233
2. K úloze státu a k limitům veřejné moci při zajištění kybernetické bezpečnosti	235
3. K českému zákonu o kybernetické bezpečnosti a k opatřením NÚKIB k zajištění kybernetické bezpečnosti	236
Seznam použité literatury	239