

Kibernetska kriminaliteta

Aleš Završnik

IUS SOFTWARE®



Založba



INŠTITUT ZA KRIMINOLOGIJO
pri Pravni fakulteti v Ljubljani

Ljubljana 2015

Uvodna beseda

Knjiga je plod večletnega spremljanja novih pojavnih oblik kriminalitete, povezane z računalniki, internetom in novimi storitvami informacijske družbe. Narava te kriminalitete je še posebej povezana s tekom časa: z novimi tehnološkimi iznajdbami na področju informacijsko-komunikacijske tehnologije vznikajo nove ali se spreminjajo obstoječe rabe ali zlorabe, ki vodijo v kriminaliteto. Bolj podrobno spremljanje tudi na področju kibernetске kriminalitete pokaže, da kvalitativnih skokov ni. Po grobi oceni drži le, da so se motivi storilcev v desetih letih, odkar smo na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani o tem področju opravili prvo raziskavo v Sloveniji, spremenili, in če smo prej govorili o zanesenjaških hekerjih, smo danes večinoma priča organiziranemu kriminalu, ki zasleduje predvsem premoženjske koristi, in državnemu kriminalu. A spremembe so evolutivne narave, zato bom predstavil razmišljanje o kibernetски kriminaliteti, ki bo bolj celovito od pogosto pretencioznih poročil tako ekspertov na področju informacijske tehnologije, ki vidijo v vsaki novi obliki grožnje »revolucionarne« in »uničujoče« spremembe, kot od senzacionalističnih medijev, ki sporadično »odkrivajo« podatke o »miliardnih izgubah« zaradi kiberkriminalcev in strašijo javnost.

Besedilo obravnava kibernetско kriminaliteto v kazenskopravni in kriminološki maniri. Pristop vključuje številne razlage pojava v socioloških terminih in kriminalitetno-politične premisleke vrednostne narave, s katerimi upošteva zakonodajne rešitve, sprejete tako na nadnacionalni ravni, na primer v aktih EU in Sveta Evrope kot na nacionalnem nivoju. Pozitivnopravni akti so večinoma predstavljeni kot primer možnih kazenskopravnih odzivov na izbrani problem. Knjiga si v tem smislu skuša zagotoviti nekoliko daljši rok trajanja; tudi ko bodo konkretne določbe kazenskega zakona že spremenjene, bo temeljna problematika ostala. Struktura knjige sledi delno kriminološkemu kanonu, ko predstavi pojem, fenomenologijo, epidemiologijo in odzivanje na to vrsto kriminalitete, delno pa sledi kazenskopravni razdelitvi na materialni in procesni del.

Knjiga nagovarja študentke in študente kriminologije, kazenskega prava in prava informacijske tehnologije, v tujini znanega področja kot IT *law* ali *cyber-law*, in praktike, delujoče v kazenskopravnem sistemu. Predvsem naslavlja družboslovno izobraženo javnost in ne zahteva tehničnega propedevtičnega znanja.

Ob tej priložnosti se zahvaljujem študentki Lauri Matjašec za pomoč pri urejanju besedila, lektorici Marinki Milenkovič, ki je neprecenljiva jezikoslovka na področju kazenskega prava in kriminologije, sodelavcem na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani za stimulatивно okolje in založniku IUS SOFTWARE, GV Založba, za prijazno pomoč pri končnih korakih, da je knjiga dosegla vas, spoštovane bralke in bralci. Knjiga je stranski produkt raziskovanja na podoktorskem projektu Tehnično okrepljeno nadzorovanje in boj zoper kriminaliteto: Etični, pravni in kriminološki vidiki porajajočih se detekcijskih in nadzornih tehnologij.

Posebej hvala vama, Ela in Mía, da me nista nikoli prav dolgo pustili sedeti za računalnikom. Morda sem se tako izognil tudi sam kakšni kibernetiski viktimizaciji.

avtor

V Ljubljani, 7. aprila 2015

Kazalo

1. Pojem kibernetške kriminalitete in sorodni pojmi	11
1.1. Kibernetška kriminaliteta	11
1.2. Kibernetška varnost	16
1.3. Kibernetški terorizem in kibernetško vojskovanje	19
2. Razvoj kibernetške kriminalitete	21
2.1. Razvoj interneta	21
2.2. Hekerska kultura	22
3. Fenomenologija kibernetške kriminalitete	24
3.1. Taksonomije kibernetške kriminalitete	24
3.2. Kibernetška kriminaliteta, povezana z integriteto informacijskega sistema in podatkov	26
3.2.1. Osnovni pojmi	26
3.2.2. Izzivi kazenskega pregona	27
3.2.2.1. Poskus dostopa oziroma vstopa v informacijski sistem	27
3.2.2.2. Pripomočki oziroma orodja, namenjena izvršitvi teh kaznivih dejanj	28
3.3. Kibernetška kriminaliteta, povezana z vsebino	29
3.3.1. Kibernetška kriminaliteta, povezana s spolnimi vsebinami	30
3.3.1.1. Obseg in osrednji izzivi kazenskopravnega odzivanja	30
3.3.1.2. Pojem »ekstremne« pornografije	32
3.3.1.3. Pojem otroške pornografije	32
3.3.1.4. Širitev boja zoper otroško pornografijo	36

3.3.2. Kibernetska kriminaliteta, povezana z nasilnimi vsebinami	37
3.3.2.1. Kibernetsko nadlegovanje	37
3.3.2.2. Kibernetska kriminaliteta, povezana s sovražnim govorom	39
3.3.3. Kibernetska kriminaliteta, povezana s kršitvijo pravic intelektualne lastnine	42
3.3.3.1. Kazensko pravo v navzkrižnem ognju industrijskih interesov	42
3.3.3.2. Škoda zaradi kršitev pravic intelektualne lastnine na internetu	43
3.3.3.3. Kazenskopravni instrumenti za varstvo pravic intelektualne lastnine	44
3.4. Kibernetska kriminaliteta, povezana z računalniki	47
4. Pojavnost kibernetske kriminalitete	54
4.1. Ocene pojavnosti	54
4.2. Metodološke dileme	56
5. Odzivanje na kibernetsko kriminaliteto	59
5.1. Splošno o zagotavljanju reda v kibernetskem prostoru	59
5.2. Jurisdikcija za kibernetska kazniva dejanja	63
5.3. Elektronski dokazi	64
5.4. Pridobivanje kibernetskih forenzičnih podatkov	65
5.4.1. Prikrit kibernetski nadzor	66
5.4.2. Pridobivanje podatkov od ponudnikov komunikacijskih storitev	66
5.4.3. Zaseg, zavarovanje in preiskovanje računalnikov in mrež	68
5.4.3.1. Posebna določila Budimpeške konvencije	69
5.4.3.2. Slovenska ureditev	72
5.5. Posebej o digitalni (računalniški in mrežni) forenziki	73
5.6. Izbrane digitalne preiskovalne metode in tehnike	77
5.7. Dokazovanje z elektronskimi dokazi pred sodiščem	81

5.8. Mednarodno sodelovanje in varstvo pred kibernetško kriminaliteto	82
5.8.1. Aktivnosti OECD, Sveta Evrope in OZN	82
5.8.2. Aktivnosti drugih mednarodnih organizacij	87
5.8.3. Aktivnosti Evropske unije	89
6. Kriminalitetna politika in kibernetška kriminaliteta	94
7. Razvoj slovenske teorije	98
8. Izbrane teme	101
8.1. Upravljanje interneta in internetne infrastrukture	101
8.2. Obveščevalna dejavnost in internet	104
8.3. Hakerstvo	107
8.4. Haktivizem in politična raba interneta	109
8.5. Nevtralnost interneta in razvoj zaprtih platform: konec interneta?	110
8.6. Kriptovalute	111
8.7. Globoki splet in temačni splet	114
8.8. Internet stvari: svetla prihodnost kibernetške kriminalitete?	115
9. Sklep	118
Literatura	121
Povzetek	137
Abstract	139
Stvarno kazalo	141
Imensko kazalo	141
Seznam slik, tabel in primerov	143
O knjigi	155

O knjigi

Monografija je nastala na podlagi spremljanja pojavnih oblik kriminalitete, ki so povezane z razvojem informacijske družbe in informacijsko-komunikacijskih tehnologij. Poleg predstavitve stroke, primerov in razvojnih sprememb opiše posamezne pojavnne oblike, naveže pa se tudi na pravodajne rešitve in zakonodajo za potrebe kazenskega pregona kibernetске kriminalitete. Avtor nagovarja praktike na kazenskopravnem področju in študente; razumljivo in preprosto, a vseeno na visoki ravni predstavlja področje družboslovno izobraženi javnosti. To ni še ena izmed klasičnih knjig o kibernetски kriminaliteti, obravnavani s »klasičnega«, tehničnega vidika, pač pa inovativno delo, ki razumljivo predstavlja kibernetско kriminaliteto tehnično neizobraženim bralcem. Zato je zelo pomembna za razumevanje in nadaljnji razvoj področja.

Avtor opredeli pojem kibernetске kriminalitete in z njim povezane pojme, oriše njen razvoj, z opisom fenomenologije pojasni izzive kazenskega pregona in vlogo sodobne informacijsko-komunikacijske tehnologije. Govori o odzivanju na kibernetско kriminaliteto in o kriminalitetni politiki. Na koncu predstavi še izbrane teme, povezane s kibernetско kriminaliteto – od klasičnih oblik pridobitniško motivirane kibernetске kriminalitete do kibernetskega bojevanja in boja za informacijsko moč ter prevlado z močjo informacij – dotakne pa se tudi mejnih področij, kot je kibernetски terorizem.

Za lažje razumevanje in izvajanje podpore v organizacijah so opisani splošni in konceptualni vidiki zlorab kibernetskega prostora in pravne podlage za razumevanje pojava s pravnega stališča. Vidiki so smiselno (po)razdeljeni na posamezna poglavja, opisane so razlike med obravnavanimi področji ter podane primerjave posameznih oblik kibernetске kriminalitete.

Knjigo priporočam vsem, ki se srečujejo s kibernetско kriminaliteto in jo želijo razumeti z netehničnega vidika. Za globlje razumevanje tehničnega

dogajanja je na voljo več drugih knjig, čeprav žal ne v slovenščini. Avtor s svojim delom prispeva k razumevanju tega področja z vidika naše zakonodaje in vpetosti Slovenije v mednarodne tokove.

doc. dr. Igor Bernik

Fakulteta za varnostne vede Univerze v Mariboru

Knjigo doc. dr. Aleša Završnika sem vzel v roke poln pričakovanj. Razloga za to sta bila dva: prvič, ker gre za avtorja, ki že vrsto let suvereno krmari med čermi digitalnega sveta; in drugič, ker gre za delo, ki ga (zdaj že globoko) v 21. stoletju nujno potrebujemo tudi v slovenskem okolju. Pričakovanja je avtor brez dvoma upravičil. Pred nami je knjiga, ki kaže avtorjevo edinstveno sposobnost živjeti se v multidisciplinarni kriminološki diskurz, pri čemer vendarle sledi ustaljenim smernicam kriminološke sistematike; tako ima delo vse značilnosti znanstvene monografije. Branje je polno izzivov, ki premikajo meje bralčevega razumevanja svetovnega spleta.

Avtor je v preteklosti že večkrat črpal iz multidisciplinarne zakladnice kriminološke znanosti. Tudi ta knjiga je, metodološko, sinteza pravnih, socioloških, kulturoloških in psiholoških pristopov, oplemenitenih s prvini računalništva in informatike. Kompleksnost predmeta preučevanja, kibernetika kriminaliteta, takšen pristop ne le upravičuje, ampak ga zahteva. Brez tega bi se avtorjev spopad s tem kompleksnim pojavom gotovo klavrno končal. Tako pa besedilo spretno usmerja bralca od pravnih vidikov nacionalnih in nads nacionalnih mehanizmov upravljanja svetovnega spleta do empirije spletnega vsakdanjika, prek hekerske kulture v najtemnejše globine tehnološko zahtevnega svetovnega spleta. Morda je tu prav pojasniti: tisti, ki (še) nismo večji izrazja, specifičnega za razpravljanje o kibersvetu, bomo z zadovoljstvom ugotovili, da nas avtor dosledno skuša rešiti zadrege. Delo je opremljeno z obsežnimi sprotnimi pojasnili in pripombami, ki krepijo bralčevo razumevanje temeljnih in manj temeljnih pojmov. Posebej dragoceni za razumevanje so še predstavljene študije primerov, diagrami in ilustracije, ki hkrati razgibajo tekst in dajejo priložnost za razmislek ob branju. Kompleksnost, ki jo zahteva pisanje o kibernetiki kriminaliteti, uspe avtorju približati tistim, ki se s temi pojavi seznanjajo prvič.

K temu dodatno pripomore tudi dejstvo, da besedilo sledi ustaljeni, tradicionalni strukturi kriminoloških pregledov. Delo je mogoče razdeliti na tri

temeljne dele: opredelitev osnovnih pojmov, fenomenologijo kibernetске kriminalitete in oblikovanje odzivov nanjo. Avtorju znotraj teh sklopov pogosto služi kot izhodišče Budimpeška konvencija (Konvencija o kibernetски kriminaliteti), tako kot drugim avtorjem temeljnih del s tega področja. Rezultat je pregledna, sistematična in izčrpna sinteza, ki vodi bralca od splošnega k posebnemu, poleg tega pa razčlenjuje posamezne gradnike mozaika kibernetске kriminalitete in z njo povezanih pojavov. Posebno dodano vrednost ima osmi del knjige, ki je posvečen izbranim temam in vprašanjem. V tem delu bo bralec našel nova izhodišča za preučevanje spletne realnosti. S tem na eni strani avtor ponudi nabor aktualnih spletnih družbenih pojavov, na drugi strani pa izhodišča za nadaljnja kriminološka raziskovanja.

Če na koncu dodamo še obsežen znanstveni aparat ter avtorjev zgoščen, dinamičen in suveren pristop, ugotovimo, da imamo pred seboj monografijo, ki zaokrožuje dosedanje delo slovenske pravne in kriminološke stroke. Po njej bomo posegli vsi, ki nas bo pot zanesla v preučevanje in poučevanje kibernetске kriminalitete. In to bo, verjemite, vedno pogosteje.

doc. dr. Primož Gorkič
Pravna fakulteta Univerze v Ljubljani