Igor Bernik: Cybercrime and Cyberwarfare, (Focus Series). London: ISTE; Hoboken: Wiley, 2014

V Sloveniji smo v zadnjem obdobju priča katastrofalnim naravnim nesrečam in zdi se, da se te vrstijo čedalje pogosteje, skorajda vsako leto. Posebne razmere, ki nastopijo zaradi naravnih pojavov, vplivajo na kritično infrastrukturo družbe in brez dvoma tudi na delovanje informacijskih tehnologij. Šele ko je večje število prebivalcev Slovenije nekaj dni ostalo brez elektrike, smo se začeli resneje spraševati o pomenu vsakdanje tehnologije in naši odvisnosti od nje.

Kakšen pomen ima za človeka današnja tehnologija in kaj se zgodi, ko nam jo je onemogočeno uporabljati? Takoj se pokažejo ranljivosti sistemov, priložnosti uresničitve groženj informacijskim sistemom, možnosti za delovanje kibernetskih kriminalcev in celo za kibernetsko vojskovanje. Zato je knjiga doc. dr. Igorja Bernika (v nadaljevanju avtor) *Cybercrime and Cyberwarfare* še posebej aktualna. Knjiga je januarja 2014 izšla pri ugledni mednarodni založbi Willey. Pomembnost in aktualnost tematike dela se kažeta tudi v dostopnosti knjige na svetovnih knjižnih portalih.

Avtor v omenjenem delu opisuje področji, ki združujeta človeške oz. družbene dejavnike z dogajanjem v kibernetskem prostoru: kibernetsko kriminaliteto in kibernetsko bojevanje. Tako kibernetska kriminaliteta kot kibernetsko bojevanje postajata pereč problem številnih posameznikov, podjetij, vladnih in nevladnih organizacij v svetu in Sloveniji. Zato je to delo še toliko bolj pomembno, saj celovito in na razumljiv način obravnava posamezna področja obeh omenjenih pojavov ter poudari glavne pomanjkljivosti na tem področju: šibko mednarodno sodelovanje in posledično počasno skupno odzivanje in preprečevanje.

Avtor omogoča bralcu vpogled v svet kibernetske kriminalitete in kibernetskega bojevanja. To je svet, ki ga, kot vemo, ne omejujejo državne meje. Omenjena pojava ne opisuje s tehničnega vidika, ampak tako, da razširi bralčevo razumevanje vplivov kibernetske kriminalitete in kibernetskega bojevanja na zagotavljanje celovite informacijske varnosti v organizacijah. Opisani so tako splošni kot konceptualni vidiki zlorab kibernetskega prostora, ki so logično in smiselno (po)razdeljeni v področje kibernetske kriminalitete in kibernetskega bojevanja. Prikazane so razlike med kibernetsko kriminaliteto in kibernetskim bojevanjem, delovanje storilcev ter način preiskovanja in zoperstavljanja napadom kibernetskih storilcev, odzivanje na incidente ter ne nazadnje tudi potrebni ukrepi za izboljšanje stanja. Vse posamezne tematike avtor v nadaljevanju podrobno razdela.

V prvem delu knjige avtor obravnava kibernetsko kriminaliteto, ki jo odlično opiše z vidika storilcev, preiskovalcev in žrtev tovrstne kriminalitete. Omenjena so tudi orodja za izvajanje kibernetskih napadov, vendar delo ne obravnava tehničnih vidikov, saj avtor zapiše, da je del o tehnologiji omenjenega področja dovolj, njegov namen pa je poučiti bralca z družbenega in organizacijskega vidika kibernetske kriminalitete. V nadaljevanju avtor predstavi oblike zaščite pred kibernetskimi napadi, strah uporabnikov pred kibernetskim napadom, metode preiskovanja in stroške odpravljanja posledic kibernetske kriminalitete. Na koncu poglavja omeni tudi mednarodne vidike kibernetske kriminalitete in mednarodno usklajene pravne akte za pregon globalne kibernetske kriminalitete, ki ne pozna in ne priznava državnih meja.

Drugi del knjige je namenjen obravnavi kibernetskega bojevanja. Za začetek avtor pojasni razliko med klasično kibernetsko kriminaliteto in dejanji, ki potekajo v sodobnem kibernetskem prostoru in jih uvrščamo v področje kibernetskega bojevanja. Zatem odgovarja na vprašanja, kdo je vpleten v kibernetsko bojevanje, kakšni so motivi storilcev, kdo so njihove žrtve. Avtor podrobno opiše tudi vlogo nekaterih držav, ki so tako ali drugače vpletene v kibernetsko bojevanje. Kot najmočnejši na tem področju izpostavi ZDA in Kitajsko, sledijo Severna Koreja, Rusija in Indija, ki konkurirajo najmočnejšim ter mali Izrael, ki ima nesorazmerno velik vpliv, tudi zaradi pomoči ZDA in Evrope. Omenjene so tudi države, ki imajo pomembno vlogo v omejevanju kibernetskega bojevanja, tako na nacionalni kot nadnacionalni oz. svetovni ravni, saj kot zapiše avtor, se je potrebno pri zoperstavljanju opreti na lastne sile, če pa želi posamezna država omejiti vplive napadov, mora biti sposobna tudi napasti nasprotne države. Tega, kot je zaradi s Snowdnom povezanimi dogodki zdaj znano tudi nepoznavalcem, se poslužujeta v največji meri ZDA in Kitajska, pa tudi Rusija bistveno ne zaostaja.

Ob koncu avtor izpostavi skupne točke kibernetske kriminalitete in kibernetskega bojevanja. Na podlagi skrbnih analiz obravnavanih področij avtor navede metode, ki se uporabljajo za zaščito pred kibernetsko kriminaliteto in kibernetskim bojevanjem, tako na ravni posameznika kot na ravni organizacij in držav. Predlaga smernice razvoja na obravnavanih področjih; mednarodno sprejete pravne akte, izboljšanje mednarodnega sodelovanja, premik v glavah odgovornih od nacionalnega v globalno in splošno zaščito informacijskih sistemov na višjem nivoju. Predstavitev tematike zaokroži z metodami zaščite, ki jih moramo upoštevati vsi uporabniki, tako posamezniki, organizacije kot tudi države s svojimi institucijami, da se zavarujemo pred kibernetskimi napadi. Glede tega avtor posebej izpostavlja pomembnost človeškega dejavnika, predvsem pomen izobraževanja ljudi o nevarnostih kibernetskega prostora, možnostih zaščite v njem, pametnem načinu uporabe informacijske tehnologije ter varnem delovanju uporabnikov v kibernetskem prostoru.

Fakulteta za varnostne vede doslej še ni imela knjige s poglobljeno obravnavo kibernetske varnosti, kibernetske kriminalitete in kibernetskega bojevanja v angleškem jeziku, zato je delo doc. dr. Igorja Bernika pomemben prispevek k širši prepoznavnosti fakultete pri njenem delovanju na različnih področjih informacijske varnosti. Knjiga predstavlja pomemben mejnik v razumevanju in celovitosti pogleda na obravnavano tematiko in je pomembno gradivo pri

načrtovanju smernic razvoja informacijske varnosti ter nadaljnjega raziskovanja te tematike. Izid knjige pri svetovno priznani založbi Willey pa ne pomeni samo veliko priznanje avtorju, ampak krepi tudi ugled Fakultete za varnostne vede in Univerze v Mariboru na področju proučevanja kibernetske varnosti.

Blaž Markelj