VARSTVOSLOVJE,
let. 15
št. 3
str. 317–337

Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje

Aleksandar Ilievski, Igor Bernik

Namen prispevka:

Številna poročila mednarodnih in nacionalnih organizacij iz zadnjega obdobja govorijo o hitrem in inovativnem razvoju kibernetske kriminalitete. V tem prispevku želimo analizirati organiziranost in način boja proti kibernetski kriminaliteti v Sloveniji, proučiti pravne podlage za to področje in predstaviti nacionalne statistične podatke o njenem uresničevanju.

Metode:

Splošne ugotovitve so oblikovane na podlagi pregleda literature, pregleda dejavnosti v Republiki Sloveniji, javnih, zasebnih in mednarodnih organizacijah, povezanih s kibernetsko in informacijsko varnostjo, pregleda zakonodaje ter dostopnih uradnih statističnih podatkov o kibernetski kriminaliteti.

Ugotovitve:

Ključno vlogo pri preiskovanju kibernetske kriminalitete v Sloveniji imajo Center za računalniško preiskovanje, Slovenski center za posredovanje pri omrežnih incidentih (SI-CERT) in Evropski center za kibernetsko kriminaliteto. V boj proti kibernetski kriminaliteti so vključene tudi druge državne, nepolicijske organizacije, zasebna informacijsko-varnostna podjetja, nevladne in mednarodne organizacije. Pravna podlaga za boj proti kibernetski kriminaliteti v Sloveniji je napredna in je del več nacionalnih in mednarodnih pravnih aktov. Največji problem, s katerim se srečujejo organi pregona, je redko obravnavanje kibernetskih kaznivih dejanj v globalnem razcvetu kibernetske kriminalitete, saj smo imeli v Sloveniji v zadnjih sedmih letih le nekaj obsodilnih obsodb.

Omejitve/uporabnost raziskave:

Prispevek proučuje boj proti kibernetski kriminaliteti v Sloveniji, vključujoč mednarodne organizacije, ki delujejo na območju države.

Izvirnost/pomembnost prispevka:

Na državni ravni še niso bili analizirani način, organiziranost in uspešnost boja proti kibernetski kriminaliteti. V prispevku izpostavljamo probleme, s katerimi se

srečuje Slovenija, in predlagamo priporočila za uspešnejši boj proti kibernetski kriminaliteti.

UDK: 343.9:004

Ključne besede: kibernetska kriminaliteta, omejevanje, institucije, pravna podlaga, Slovenija

Combating Cybercrime in Slovenia: Organization, Method, Legal Basis and its Implementation

Purpose:

Numerous recent reports by international and national organizations talk about the rapid and innovative development of cybercrime. In this paper we would like to analyze the structure and method of combating cybercrime in Slovenia, examine the legal basis regarding this field and present national statistics on its implementation.

Methods:

The general findings are reported on the basis of literature, reviews of the activities of individual state, public, private and international organizations related to cyber and information security, reviews of laws and further available official statistics in the field of cybercrime.

Findings:

The Center for computer investigation, SI-CERT and the European cybercrime center play a key role in the investigation of cybercrime in Slovenia. Additional non-police government organizations, private information-security companies, NGOs and international organizations are also included in the fight against cybercrime. The legal basis for the fight against cybercrime in Slovenia is advanced and is part of several national and international acts. The biggest problem faced by the law enforcement authorities is a rare approach to cyber criminal offenses during the global boom in cybercrime. For instance, there were only a few condemnatory convictions in Slovenia in the last seven years.

Research Limitations/Implications:

The paper examines the combat against cybercrime in Slovenia, including international organizations which are operating in the country.

Originality/Value:

The exact method, the organization and level of success of the fight against cybercrime have not yet been analyzed within a national framework. In this paper, we highlight the problems which Slovenia faces, and recommend more effective methods to fight against cybercrime.

UDC: 343.9:004

Keywords: cybercrime, limiting, institutions, legal basis, Slovenia

1 UVOD

Mednarodne in nacionalne organizacije beležijo hitro naraščanje števila kibernetskih napadov. Razvoj informacijsko-komunikacijskih naprav in njihovo spletno povezovanje ter gospodarska nestabilnost in neozaveščenost spletnih uporabnikov dodatno povečujejo možnosti škodljivih kibernetskih dejanj. Svetovni splet je na voljo tako običajnim spletnim uporabnikom kot tudi storilcem kaznivih dejanj v kibernetskem prostoru, ki z izkoriščanjem »odvisnosti« uporabnikov od spleta uresničujejo svoje cilje. Storitve, kot so nakupovanje, plačevanje blaga in storitev, pošiljanje datotek, elektronsko bančništvo, prenos podatkov in druge oblike poslovanja, ki potekajo prek interneta, povezovanje z mobilnimi napravami ter neomejen dostop in povezanost globalnega kibernetskega prostora, so sčasoma postale samoumevne in vsakdanje (Bernik in Prislan, 2012).

Boj proti kibernetski kriminaliteti je kompleksen, zato se organi pregona brez sodelovanja z mednarodnimi ustanovami, zasebnim sektorjem ter širšo javnostjo ne morejo uspešno boriti proti dejavnikom tovrstne kriminalitete (Brenner, 2007; Wall, 2007; Wall, 2007/2010). Specifičnost preiskovanja kibernetske kriminalitete zahteva od organov pregona poleg sodelovanja in izmenjevanja podatkov med institucijami na nacionalni in mednarodni ravni tudi dobro tehnološko opremljenost, strokovnost, poznavanje informatike in obvladovanje računalniških veščin. Institucionalna in pravna podlaga boja proti kibernetski kriminaliteti na evropski ravni sta Evropski center za kibernetsko preiskovanje, namenjen zaščiti evropskih državljanov in podjetij pred kibernetsko kriminaliteto, ki je začel delovati januarja 2013 (Europol, 2013), in Evropska konvencija o kibernetski kriminaliteti, ki državam podpisnicam daje pravno podlago za boj proti kibernetski kriminaliteti in je osnova za mednarodno sodelovanje (Rupnik, 2003).

V boj proti kibernetski kriminaliteti v Sloveniji in drugih evropskih državah so vključene številne organizacije na nacionalni in mednarodni ravni. V tem prispevku so analizirani načini, organizacija in uspešnost boja proti kibernetski kriminaliteti v Sloveniji. Predstavljamo organizacije in posameznike, ki delujejo na tem področju. Analiziramo njihovo delo, pravne podlage na nacionalni in mednarodni ravni ter uradne statistične podatke o številu kaznivih dejanj in pravnomočnih kazenskih sankcij na področju kibernetske kriminalitete.

2 KIBERNETSKA KRIMINALITETA

Kibernetski prostor ne pozna nacionalnih meja in zajema vse oblike digitalne dejavnosti. Zaradi kompleksnosti področja in različnih pogledov posameznih držav (še) nimamo univerzalno sprejete definicije kibernetske kriminalitete, čeprav so ta pojem do zdaj poskušale opredeliti številne organizacije in avtorji. Ob upoštevanju elementov, kot jih definira Konvencija o kibernetski kriminaliteti, jo Bernik in Meško (2011: 243) definirata kot: »Kibernetska kriminaliteta pomeni uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih dejanj.« Avtorja upoštevata tudi škodljiva in nemoralna dejanja v kibernetskem prostoru, ki niso nujno kriminalna in kazniva. Tudi Wall (2007: 28) pravi, da ni nujno, da

so dejanja inkriminirana in kibernetsko kriminaliteto definira kot »kazniva in škodljiva dejanja, ki vključujejo pridobitev ali manipulacijo s podatki zaradi določene koristi«. Na desetem kongresu organizacije Združenih narodov o preprečevanju kriminalitete in ravnanju s storilci (United Nations, 2000) je bila na delavnici, posvečeni kriminaliteti, povezani z računalniškimi omrežji, kibernetska kriminaliteta definirana v ožjem in širšem pomenu besede. V ožjem pomenu je kibernetska kriminaliteta »vsak protipravni način dela, ki se upravlja elektronsko in katerega cilj je motenje varnosti računalniških sistemov in podatkov, ki jih ta sistem obravnava«. Kibernetska kriminaliteta v širšem pomenu besede pa je definirana kot »vsako protipravno dejanje, ki se izvaja prek računalniških sistemov ali omrežja ali je kakor koli povezano z njimi.« V definicijo kibernetske kriminalitete se vključuje tudi uporaba računalnikov za izvajanje kaznivih dejanj. Dashora (2011: 240) definira kibernetsko kriminaliteto kot »kriminal, storjen na spletu, pri čemer se računalnik uporablja kot sredstvo ali cilj napada«. Tudi nekateri drugi (npr. Wilson, 2008; Yazdanifard, Oyegoke in Seyedi, 2011) podobno definirajo kibernetsko kriminaliteto.

V zadnjih letih so postale nelegalne in škodljive dejavnosti v kibernetskem prostoru zelo organizirane in inovativne (Bernik in Meško, 2011). Zato lahko na podlagi škode, števila storilcev kaznivih kibernetskih dejanj in njihovih žrtev govorimo o zelo uspešnem poslovanju (Anderson et al., 2012; Norton, 2011, 2012). Enotna univerzalna definicija, ki bi dala temeljna izhodišča za nadaljnje delo in poenotenje mednarodnega boja proti kibernetski kriminaliteti, je potrebna zaradi internacionalizacije problema in morebitne nevarnosti.

3 BOJ PROTI KIBERNETSKI KRIMINALITETI

Narava kibernetskega prostora in transnacionalnost kibernetskih dejanj sta zadosten izziv in pokazatelj kompleksnosti preprečevanja in zatiranja tovrstne kriminalitete. Zaradi potrebe po tehnološki opremljenosti, strokovnosti, znanjih o informatiki in obvladovanju računalniških veščin med preiskovalci kaznivih dejanj ter potrebe po mednarodnem sodelovanju in sodelovanju drugih vladnih in nevladnih organizacij in širše javnosti je boj proti kibernetski kriminaliteti bistveno bolj zapleten kot boj proti konvencionalni kriminaliteti (Bernik in Prislan, 2012; Broadhurst, 2006; Burns, Whitworth in Thompson, 2004; Wall, 2007).

Nadzor nad kriminaliteto, ki vključuje uporabo digitalne tehnologije in računalniškega omrežja, nalaga vzpostavljanje in delovanje novih mrež. Sem spadajo povezave med policijo in drugimi vladnimi organi, povezave med policijo in nepolicijskimi javnimi in zasebnimi organizacijami (npr. CERT in ISP), povezave med policijo in mednarodnimi organizacijami (npr. Europol-EC3, ENISA, Eurojust, CEPOL) ter povezava med policijo in spletnimi uporabniki (Brenner, 2007; Broadhurst, 2006; Wall, 2007, 2007/2010). (Ne)učinkovitost organov pregona je odvisna od številnih dejavnikov, kot so pomanjkanje standardne definicije kibernetske kriminalitete, težave pri preiskovanju kibernetske kriminalitete, nezmožnost pridobivanja in vzdrževanja tehnologije, potrebne za preiskovanje kaznivih dejanj zaradi velikih stroškov, težave z usposabljanjem zaposlenih

in pridobivanjem vodstvenih kadrov, zadolženih za preiskovanje, neustrezna zakonodaja itn. (Bossler in Holt, 2012; McQuade, 2006; Stambaugh et al., 2001). Empirične raziskave, opravljene med pripadniki organov pregona, zadolženimi za boj proti kibernetski kriminaliteti, kažejo, da organi pregona dejansko raziščejo zelo malo primerov kibernetske kriminalitete (Hinduja, 2004; Senjo, 2004; Stambaugh et al., 2001) in opozarjajo na pomanjkanje znanja, veščin in sposobnosti zaposlenih, pa tudi na pomanjkanje ustreznih tehničnih sredstev za preiskovanje tovrstne kriminalitete (Bossler in Holt, 2012; Burns et al., 2004; Davis, 2012; Hinduja, 2004; Holt, Bossler in Fitzgerald, 2010; Stambaugh et al., 2001). Navedene težave organov pregona omogočajo storilcem, da se kaznivih dejanj lotevajo brez strahu, kar povečuje »temno polje« njihovega delovanja.

Evropske države imajo zaradi razmeroma poenotenih standardov podoben način delovanja pri zatiranju in preprečevanju kibernetske kriminalitete. V Evropski uniji deluje več organizacij za mednarodno sodelovanje in izmenjavo podatkov. V Sloveniji boj proti kibernetski kriminaliteti poteka prek različnih nacionalnih in mednarodnih akterjev, ki različno vplivajo na povečanje nadzora nad kibernetskim okoljem.

4 BOJ PROTI KIBERNETSKI KRIMINALITETI V SLOVENIJI

Preden začnemo razpravo, bomo prikazali akterje, ki sodelujejo v boju proti kibernetski kriminaliteti v Sloveniji. Prikaz na sliki 1 je narejen na podlagi pregleda literature (Brenner, 2007; Enisa, 2011; Europol, 2013; Policija, 2010; RAND Europe, 2012; SI-CERT, 2013; Wall, 2007/2010) in poznavanja slovenskega prostora v boju proti kibernetski kriminaliteti.

4.1 Uprava kriminalistične policije

Policija kot državni organ, zadolžen za vzdrževanje reda in uveljavljanje nacionalne zakonodaje, ima v boju proti kibernetski kriminaliteti majhno, vendar pomembno vlogo (Wall, 2007/2010). Vloga policije se razlikuje od primera do primera. Pri svojem delu, torej preiskovanju domnevnih kršiteljev in zbiranju dokazov, policija običajno kombinira tradicionalne policijske metode z uporabo računalnikov (Sommer, 2004). Število tovrstnih kaznivih dejanj narašča pri nas in po svetu. Na področju preiskovanja kibernetske kriminalitete in računalniške forenzike slovenska kriminalistična policija usmerjeno deluje od leta 1999 (Policija, 2010). Leta 2009 je kriminalistična policija na novo organizirala to področje in ustanovila Center za računalniško preiskovanje ter štiri regijske oddelke (SKP Koper, Ljubljana, Celje in Maribor). V njih so zaposleni kriminalisti z odličnim znanjem informatike in računalništva, ki zaradi hitrega razvoja informacijske tehnologije (predvsem strojne in programske opreme) ter vedno novih načinov izvrševanja kaznivih dejanj skrbijo tudi za redno posodabljanje opreme (Strniša, 2010).

Računalniško preiskovanje obsega preprečevanje, odkrivanje, preiskovanje in dokazovanje kaznivih dejanj v kibernetskem prostoru in kaznivih dejanj, storjenih

Slika 1: Shematski prikaz organiziranosti boja proti kibernetski kriminaliteti v Sloveniji

z računalniško tehnologijo, ter zavarovanje računalniških podatkov, ki lahko kažejo na kazniva dejanja (Svetek in Kebe, 2003). Center in oddelki za računalniško preiskovanje pokrivajo tri glavna področja dela (Policija, 2010):

- preiskovanje kaznivih dejanj računalniške kriminalitete (zloraba osebnih podatkov, kršitev materialnih avtorskih pravic, napad na informacijski sistem, vdor v poslovno-informacijski sistem ter izdelovanje in pridobivanje pripomočkov, namenjenih izvedbi kaznivega dejanja);
- preiskave zaseženih e-naprav oz. e-podatkov (t. i. računalniška forenzika);
- strokovna pomoč pri preiskovanju drugih področij kriminalitete (kazniva dejanja otroške pornografije, spletne goljufije, rasne nestrpnosti na internetu, davčne utaje, korupcija, zlorabe e-bančništva itd.).

Toni Kastelic, vodja Centra za računalniško preiskovanje, pravi, da so pristop in metode preiskave odvisni predvsem od vrste kaznivega dejanja, načina storitve, informacij, ki so dosegljive forenziku, in tudi od tipa elektronske naprave. Najpogostejši prvi korak pri preiskovanju je izdelava istovetne kopije celotnega nosilca podatkov oz. tako imenovane forenzične kopije podatkov, kjer se nosilec podatkov kopira v celoti, od prvega do zadnjega bita. Pri izdelavi kopije se izračunajo kontrolne vrednosti, ki zagotavljajo integriteto kopiranih podatkov, torej istovetnost kopije z izvirnikom. Forenzik nato opravi forenzično analizo oz. preiskavo, katere cilj je odkritje digitalnih dokazov, in na koncu naredi zapisnik (Intervju s Tonijem Kastelicem …, 2012).

Hiter razvoj informacijske tehnologije zahteva sprotno in intenzivno izobraževanje ter dobro poznavanje računalniške programske in strojne opreme in novih pojavnih oblik kibernetske kriminalitete, njihovega odkrivanja in poznejšega

analiziranja (Broadhurst, 2006; Burns et al., 2004; Davis, 2012; Wall, 2007/2011). Ti dejavniki lahko močno vplivajo na učinkovitost dela kriminalistične policije. Slovenija je leta 2011 za povečanje zmogljivosti centra in oddelkov za računalniško preiskovanje od OLAF-a (Evropskega urada za boj proti goljufijam) prejela finančno pomoč. S projektom je slovenska policija povečala zmogljivosti regijskih enot za preiskovanje računalniške kriminalitete in izboljšala tehnično opremljenost kriminalistov, ki so bili poleg tega deležni tudi ustreznega izobraževanja. V letu 2011 sta bila izvedena nakup večje količine računalniške strojne opreme in licenc ter ustrezno strokovno usposabljanje (Policija, 2012).

4.2 Javne in zasebne nepolicijske organizacije

Javne in zasebne nepolicijske organizacije so lahko zelo koristne pri preventivnem in represivnem delovanju proti kibernetski kriminaliteti (Wall, 2007/2010). Organizacije spodbujajo oz. omogočajo mednarodno povezovanje, povečanje števila prijavljenih kibernetskih škodljivih dejanj, povečanje ozaveščenosti spletnih uporabnikov o pojavnih oblikah in potrebi po ustrezni zaščiti, kar je velika opora v boju proti kibernetski kriminaliteti.

Mednarodna organizacija CERT (Computer Emergency Response Team), ustanovljena leta 1998 na Carnegie Mellon University v Pittsburghu, je sodobna kombinacija med zasebno in javno organizacijo (Wall, 2007/2010). Od leta 1995 deluje tudi slovenski CERT (SI-CERT) – Nacionalni center za obravnavo varnostnih incidentov na internetu. CERT sprejema prijave zlorab, vdorov in okužb ter vseh drugih dogodkov, povezanih z računalniško in omrežno varnostjo. SI-CERT deluje v okviru javnega zavoda ARNES že od svoje ustanovitve (Akademska in raziskovalna mreža Slovenije)[1]. Delovanje centra je sestavljeno iz več faz (SI-CERT, 2013). Zagotovljeno je primerno delovno okolje in ustrezno usposobljeni zaposleni, ki so predpogoj za delovanje odzivnega centra. Z incidentom se začnejo konkretno ukvarjati in analizirati, ko ga zaznajo. Najpogosteje je to takrat, ko na naslov cert@cert.si prejmejo obvestilo o incidentu. Tega razvrstijo v eno od kategorij, naredijo analizo, primerno za kategorijo ali vrsto incidenta, in korelacijo med različnimi podatki o incidentu, drugimi incidenti ter sledovi, odkritimi v preiskavi. V fazi zamejitve, odstranitve in povrnitve zbirajo dokaze, omejujejo izpostavljenost sistemov in o incidentu po potrebi obvestijo skrbnike sistemov, ponudnike in druge CERT-centre. V končni fazi sledijo še sklepne dejavnosti z zbiranjem izkušenj, ki obravnavani incident povezujejo z drugimi obravnavanimi incidenti. SI-CERT se povezuje z drugimi akterji glede informacijske in omrežne varnosti doma in v tujini. Aktivno sodelujejo v evropski delovni skupini TF-CSIRT[2] in v svetovnem

1 *Javni zavod Arnes in Ministrstvo za pravosodje in javno upravo sta na podlagi sklepa vlade RS 31. maja 2010 podpisala sporazum o sodelovanju na področju informacijske varnosti. Sporazum določa, da Arnesov varnostni center SI-CERT pomaga pri vzpostavitvi vladnega Cert-centra (delovno ime Sigov-cert) in da do vzpostavitve novega centra tudi opravlja naloge koordinacije varnostnih incidentov za vse informacijske sisteme javne uprave (SI-CERT, 2013).*

2 *TF-CSIRT od leta 2000 združuje vse evropske odzivne CERT-centre.*

združenju »First« (Forum of incident response and security teams) ter v skupini nacionalnih odzivnih centrov, ki jo vodi ameriški CERT/CC (SI-CERT, 2013).

Slovenski odzivni center SI-CERT poleg opisane dejavnosti izvaja tudi projekt, ki se imenuje »Varni na internetu«. Zastavljen je dolgoročno in zajema široko področje informacijske varnosti. Dvig stopnje informiranosti o varni rabi interneta je glavni cilj projekta ozaveščanja slovenske javnosti. Njihove dejavnosti so usmerjene k doseganju ciljev (Varni na internetu, 2013): »Dvigniti stopnjo zavedanja ciljnih javnosti o različnih nevarnostih, ki so jim izpostavljene na spletu; poučiti uporabnike o varni uporabi spletnega bančništva; poučiti uporabnike o različnih oblikah spletnih prevar in jim ponuditi praktične rešitve, kako se zavarovati; ter informirati uporabnike o varstvu osebne identitete v socialnih omrežjih.«

Drugi projekt v RS je Center za varnejši internet SAFE-SI[3], ki združuje tri komponente: ozaveščanje o varni rabi interneta in novih tehnologij; telefonsko linijo za pomoč mladim in njihovim staršem, ki se znajdejo v težavah, povezanih z uporabo interneta, ter Spletno Oko − točko za anonimno prijavo nelegalnih spletnih vsebin (otroške pornografije in sovražnega govora). Dejavnosti centra so usmerjene proti štirim ciljnim skupinam: otrokom, mladostnikom, staršem in strokovnim delavcem (učiteljem, socialnim delavcem, vzgojiteljem). Cilj projekta je, da se med izbranimi ciljnimi populacijami s sprotnim zagotavljanjem preverjenih informacij in nasvetov za varno rabo novih tehnologij v Sloveniji doseže visoka stopnja ozaveščenosti o teh temah (Program Varnejši internet v Sloveniji, 2012).

V zadnjem času je veliko pozornosti usmerjene k ponudnikom internetnih storitev, ki lahko močno vplivajo na vedenje uporabnikov. Njihov vpliv je utemeljen na pravilih in pogojih, ki jih uporabniki morajo upoštevati, ter programski opremi, ki se uporablja in ki vpliva na zmanjševanje kibernetskega prestopništva (Wall, 2007). Ponudniki internetnih storitev izkoriščajo svoj položaj v komunikacijskih omrežjih in s tem ustvarjajo varnostne mehanizme na zadevnem področju. Slednji lahko zaznavajo in preprečijo različne kibernetske napade. Wall (2007/2010) pravi, da so ponudniki najbolj zanesljivi pri vzpostavljanju varnostnih sistemov v obliki filtrov SPAM. V Sloveniji deluje Sekcija slovenskih ponudnikov internetnih storitev (SISPA), kar omogoča sodelovanje in skupno reševanje problemov, povezanih z zaščito spletnih uporabnikov pred spletnimi grožnjami. Tovrstne organizacije, ki so se začele združevati tudi na mednarodni ravni (npr. Pan-European Internet Service Providers' Association), ponujajo pridobivanje pozitivnih izkušenj ter skupno iskanje načinov za uspešen boj proti kibernetski kriminaliteti.

4.3 Zasebna informacijsko-varnostna podjetja

Varen pretok informacij je danes en od osnovnih zahtev za stabilno in uspešno poslovanje organizacij. Uspešnost delovanja podjetij je v glavnem odvisna od

3 *Projekt Centra za varnejši internet SAFE-SI izvajajo Univerza v Ljubljani, Fakulteta za družbene vede, ARNES, Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga »Generalni direktorat Connect« pri Evropski komisiji in Ministrstvo za izobraževanje, znanost, kulturo in šport (Program Varnejši internet …, 2012).*

njihovega informacijskega sistema (Bernik in Prislan, 2011). Informacijska varnost je samostojna poslovna funkcija podjetja, ki jo zagotavljajo vsi zaposleni v podjetju. O tem govori načelo o obvladovanju tveganj, ki ga je treba upoštevati tudi pri krepitvi informacijske varnostne kulture; načelo pravi, da je treba razpršiti odgovornost za njeno upravljanje tako, da skrb za upravljanje ne zadeva le vodstvenih kadrov, temveč postane naloga vseh zaposlenih v organizaciji, element vsakodnevnih dejavnosti in praks, tudi tistih, ki se na prvi pogled ne zdijo povezane z varnostjo (Chevreau, 2006).

V zadnjem času se je v Sloveniji pojavilo več podjetij, ki ponujajo storitve, povezane z zaščito in varnostnim preverjanjem informacijsko-komunikacijskih sistemov. V to skupino spadajo Sistemator, Hic Salta, SGbiro, Netis, Sibit, ATR.SIS, TrendNET, HERMES SoftLab, PRORANG, Simt, Team Intell, Palsit, S&T, MegaM, Virtua, Astec, D-NET, Viris, ACROS itn. Nekatera podjetja že imajo zaposlene certificirane računalniške forenzike. Podjetja najemajo zasebne forenzike, kadar sumijo, da je prišlo do izdaje poslovnih skrivnosti, nadlegovanja na delovnem mestu, zlorabe položaja ali notranjih informacij, uveljavljanja konkurenčne klavzule ali dokončnega izbrisa podatkov s trdih diskov (Banovič, 2007). Poleg tega se navedena podjetja ukvarjajo še z izobraževanjem zaposlenih o zaščiti in uporabi preventivnih ukrepov ter ustvarjanjem celovite varnostne politike in kulture v podjetjih (Prava ideja, 2010), kar je zelo pomembno z vidika informacijske varnosti.

4.4 Spletni uporabniki

Spletni uporabniki so najbolj izpostavljeni kibernetskemu tveganju in so pogosto žrtve kibernetske kriminalitete. S svojim ravnanjem in spletno kulturo lahko vplivajo na preventivno in represivno delovanje. V tem boju sodelujejo različne skupine uporabnikov, ki delujejo na določenem področju. Tak primer je skupina Anonymus, ki je, čeprav je znana kot kriminalna skupina, leta 2011 začela s spleta odstranjevati pedofilske vsebine in javno objavljati imena pedofilov (Anonymous napadel še pedofile, 2011).

Huey, Nhan in Broll (2012) ugotavljajo, da je lahko javnost pomemben partner organov pregona in zasebnih sektorjev pri varovanju kibernetskega prostora. Pri tem navajajo tri razloge za svoje trditve. Prvič, zaradi distributivne narave spletnega sveta lahko člani družbe postanejo »oči in ušesa« za zaznavanje kriminalnih dejanj; drugič, zaradi hitrosti informacij, ki jih zbira javnost, in mobiliziranja različnih oblik koristi, do katerih pogosto dostopajo hitreje kot najboljši organi pregona. Tretjo prednost vključevanja javnosti v civilne kiberpolicijske dejavnosti po njihovem mnenju predstavlja raznolikost posameznikov in skupin, kar omogoča dostop do široke palete koristi. Spletni uporabniki lahko z uporabo zanesljivih protivirusnih programov, požarnih zidov, filtrov antiSPAM, enkripcijo podatkov itn. ter predvsem z odgovornim in zavednim ravnanjem, ki je posledica poznavanj problematike, močno zmanjšajo svojo ranljivost in pogostost pojavljanja kibernetske kriminalitete. Prijavljanje kaznivih dejanj lahko policiji poveča motivacijo v boju proti kibernetski kriminaliteti in zoži njeno »temno polje«.

4.5 Raziskovalne in druge nacionalne organizacije

Raziskave na področju kibernetske kriminalitete so lahko učinkovite pri zagotavljanju novih načinov za odpravljanje težav, s katerimi se srečujejo državne in mednarodne institucije, ki si prizadevajo za povečanje nadzora nad kibernetskim okoljem. Prav temu služijo številne raziskovalne organizacije v Sloveniji, ki pri izvajanju svojih raziskovalnih dejavnosti ugotavljajo slabosti informacijskih sistemov, motive storilcev kaznivih kibernetskih dejanj, uporabnikove šibke točke idr. ter organom pregona in drugim organizacijam predlagajo ustrezne spremembe delovanja za učinkovitejšo preventivno in represivno delovanje na tem področju.

Pri nadzoru nad kibernetskim prostorom v Sloveniji sodelujejo številne organizacije. Ena od njih je Akademska in raziskovalna mreža Slovenije (ARNES) kot javni zavod, ki zagotavlja omrežne storitve raziskovalnim, izobraževalnim in kulturnim organizacijam, omogoča njihovo povezovanje in medsebojno sodelovanje ter sodelovanje s sorodnimi organizacijami v tujini (Arnes, 2012). Poleg ARNES-a se z raziskovanjem ukvarjajo tudi nekatere fakultete in inštituti (na primer Inštitut za informatiko, Laboratorij za telekomunikacije in Laboratorij za sistemske raziskave in informacijske tehnologije, Institut Jožef Stefan, Fakulteta za varnostne vede; Fakulteta za družbene vede, Fakulteta za elektrotehniko, računalništvo in informatiko itn.).

Naj omenimo še druge nacionalne organizacije, katerih dejavnosti so tudi zaščita in varovanje informacijskih, komunikacijskih in telekomunikacijskih omrežij. Te organizacije so (povzeto po Enisa, 2011): Informacijski pooblaščenec; Ministrstvo za visoko šolstvo, znanost in tehnologijo, Direktorat za informacijsko družbo; Ministrstvo za zunanje zadeve, Oddelek za informacijsko varnost in komunikacije; Agencija za pošto in elektronske komunikacije (APEK); Slovenska obveščevalno-varnostna agencija (SOVA); Ministrstvo za javno upravo, Direktorat za e-upravo in upravne procese; Urad Vlade RS za varovanje tajnih podatkov (UVTP) itn. Slovenija si z navedenimi organizacijami na državni in mednarodni ravni prizadeva uresničiti področno zakonodajo ter omogočiti spletnim uporabnikom varen kibernetski prostor.

4.6 Mednarodne organizacije za policijsko in pravosodno sodelovanje

Mednarodne policijske, pravosodne in druge organizacije so zaradi mednarodnega vidika kibernetske kriminalitete ključnega pomena. V Evropi delujejo štiri večje agencije za policijsko in pravosodno sodelovanje na področju kibernetskega (in drugega) prostora: Europol, ENISA, Eurojust in CEPOL, ki so v izjemno veliko oporo državam članicam pri njihovem boju proti čezmejni in organizirani kriminaliteti.

Europol je kot največja evropska policijska organizacija pristojen za reševanje hujših in organiziranih kaznivih dejanj na evropski ravni. Z zbiranjem in analiziranjem obveščevalnih podatkov, forenzično dejavnostjo in drugimi ukrepi pomaga državam članicam pri kazenskem pregonu (RAND Europe, 2012). V okviru

Europola od 11. januarja 2013 deluje Evropski center za kibernetsko kriminaliteto (EC3). Center ponuja delovno, tehnično in forenzično podporo državam članicam s strateško analizo. Cilj analize je učinkovitejše preprečevanje kibernetske kriminalitete, izboljšanje učinkovitosti kazenskega pregona, sodelovanje zasebnega sektorja v EU in določitev primerov dobre prakse ter ovir na poti k učinkovitejšemu mednarodnemu sodelovanju (Europol, 2013).

Evropska agencija za varnost omrežja in informacij (ENISA) je druga agencija, ki deluje na evropski ravni in je središče omrežne in informacijske varnosti EU, njenih držav članic, zasebnega sektorja in evropskih državljanov. V sodelovanju s temi skupinami izdaja agencija nasvete in priporočila o dobrih praksah informacijske varnosti, pomaga državam članicam pri izvajanju zadevne evropske zakonodaje ter si prizadeva za povečanje odpornosti evropske kritične informacijske infrastrukture in omrežij (Enisa, 2012).

Eurojust kot evropski pravosodni organ si prizadeva za izboljšanje učinkovitosti nacionalnih organov, pristojnih za preiskavo in kazenski pregon, pri obravnavi težjih oblik čezmejne in organizirane kriminalitete ter zagotavlja hitro in učinkovito sodno obravnavo storilcev kaznivih dejanj (Eurojust, 2012). Cilj delovanja organa je izboljšanje sodelovanja med evropskimi pravosodnimi organi in prek njih povezav z Europolom, kar vpliva na poenotenje pravosodnih standardov. Kazniva dejanja kibernetske kriminalitete obravnava Eurojustov oddelek za gospodarsko in finančno kriminaliteto (RAND Europe, 2012). Poleg navedenih organizacij na evropski ravni deluje tudi mednarodna organizacija CEPOL, namenjena usposabljanju delavcev, ki delajo na srednjih ali višjih ravneh v organih pregona na evropski ravni[4]. V CEPOL-u so do leta 2012 izvedli deset dejavnosti, povezanih s kibernetsko kriminaliteto, v katerih je sodelovalo 236 oseb (RAND Europe, 2012).

V boju proti kibernetski kriminaliteti je poleg evropskih organizacij za policijsko in pravosodno sodelovanje prisotna še svetovna mednarodna organizacija Interpol, ki izvaja tudi dejanja, povezana s kibernetsko kriminaliteto. Interpolov program dela, ki je usmerjen v boj proti kibernetski kriminaliteti, je namenjen usposabljanju in spremljanju kibernetskih groženj. Njegovi cilji so spodbujanje izmenjave informacij med državami članicami, izvajanje usposabljanja za uveljavitev in vzdrževanje kibernetskih standardov, usklajevanje in pomoč pri izvajanju mednarodnih operacij, pomoč državam članicam v primeru kibernetskih napadov, razvoj strateških partnerstev z drugimi mednarodnimi organizacijami itn. (González, 2008).

5 USKLAJENOST MEDNARODNE ZAKONODAJE, NACIONALNA PRAVNA PODLAGA IN NJENO IZPOLNJEVANJE

Države z mednarodnimi in nacionalnimi pravnimi viri varujejo državljane pred škodljivimi vplivi digitalne družbe ter organom pregona omogočajo legalen boj

4 *Med 18. in 21. oktobrom 2011 je na Brdu pri Kranju potekal seminar CEPOL o kibernetski kriminaliteti (Uprava kriminalistične policije, 2011).*

proti kibernetski kriminaliteti. Prvi mednarodni pravni akt in pravni mehanizem za mednarodno sodelovanje pri kazenskem pregonu in poenotenju nacionalnih zakonodaj je Konvencija Sveta Evrope o kibernetski kriminaliteti[5] iz leta 2001 (Broadhurst, 2006). Konvencijo je 24. julija 2002 podpisala tudi Republika Slovenija (Council of Europe, 2013). Cilj konvencije je ustvariti skupno politiko držav podpisnic, ki bo varovala družbo pred kibernetsko kriminaliteto, med drugim tudi s sprejetjem ustrezne zakonodaje in spodbujanjem mednarodnega sodelovanja (Bernik in Prislan, 2012). Konvencija je vsebinsko razdeljena na štiri poglavja (Rupnik, 2003: 2–3): v prvem delu je opredeljen pomen nekaterih za razumevanje konvencije ključnih izrazov, drugo poglavje obravnava materialno in procesno kazenskopravno problematiko, tretje opredeljuje posamezne smernice mednarodnega sodelovanja, končne določbe v četrtem delu pa določajo načine podpisa, sprejetja in veljavnosti konvencije[6]. Kmalu zatem, ko je konvencijo o kibernetski kriminaliteti 8. septembra 2004 ratificiral državni zbor (Council of Europe, 2013), je Slovenija vključila smernice konvencije v svojo nacionalno zakonodajo. V Sloveniji veljajo poleg konvencije še drugi mednarodni pravni akti, ki se nanašajo na kibernetsko kriminaliteto, kot sta Konvencija WIPO o avtorskih pravicah[7] in Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin[8] ter drugi normativni akti, ki jih je podpisala RS in se lahko uporabijo v boju proti oz. za pregon kibernetske kriminalitete.

Kazenskopravni okvir zaščite in kibernetske varnosti državljanov je vsebovan v najpomembnejšem državnem pravnem aktu, torej v Ustavi Republike Slovenije (2006). Gre predvsem za varovanje človekovih pravic in temeljnih svoboščin, ki jih ogrožajo sodobne škodljive programske kode[9]. V slovenski kazenskopravni ureditvi so kazniva dejanja v kibernetskem prostoru regulirana s Kazenskim zakonikom Republike Slovenije. Kazenski zakonik obravnava vsa inkriminirana dejanja kibernetske kriminalitete. Kljub pogostemu spreminjanju evropske in slovenske zakonodaje o kibernetski kriminaliteti še vedno obstajajo nekatera

5 *Do konca leta 2012 je Evropsko konvencijo o kibernetski kriminaliteti podpisalo in ratificiralo 38 držav, tudi države, ki niso članice Sveta Evrope (ZDA, Japonska in Avstralija) (Council of Europe, 2013).*

6 *Konvencija določa tudi številne postopkovne pristojnosti, kot so iskanje in prestrezanje vsebine na računalniških omrežjih, in je vsebinsko razdeljena na (Bernik in Prislan, 2012) kazniva dejanja zoper zaupnost, integriteto in dostopnost računalniških podatkov in sistemov (vdor v računalniški sistem, protipravno prestrezanje in motenje podatkov ter sistemov, zloraba naprav) in kazniva dejanja, povezana s samim računalnikom (računalniško ponarejanje, računalniška goljufija, kazniva dejanja, povezana z otroško pornografijo, kazniva dejanja, povezana s kršitvijo avtorskih in sorodnih pravic).*

7 *Konvencija WIPO o avtorskih pravicah, imenovana tudi Internetna pogodba, temelji na Bernski konvenciji, najpomembnejši pogodbi mednarodnega avtorskega prava. Svetovna (univerzalna) konvencija o avtorskih pravicah (1952) je v Sloveniji začela veljati 5. novembra 1992 (Bogataj Jančič, 2008).*

8 *Konvencija WIPO o avtorskih pravicah je v Sloveniji začela veljati 28. junija 1994 (Kalčina, 2005).*

9 *Ustava Republike Slovenije (2006) v 35. členu – varstvo pravic zasebnosti in osebnostnih pravic; 37. členu – varstvo tajnosti pisem in drugih občil; 39. členu – varstvo osebnih podatkov in 60. členu – pravice iz ustvarjalnosti.*

nemoralna in škodljiva dejanja, ki niso kriminalizirana in kazniva[10]. Dejstvo je, da se tehnologija razvija hitreje kot pravo, vendar, kot pravi Peršak (2009: 196), je »prepoved tehnoloških iznajdb rešitev, ki ni sprejemljiva z vidika legitimnosti kriminalizacije«. Pomembni členi kazenskega zakonika z vidika kibernetske kriminalitete so (Kazenski zakonik [KZ-1-UPB2], 2012):

- 108. člen KZ-1-UPB2: terorizem;
- 139. člen KZ-1-UPB2: kršitev tajnosti občil;
- 140. člen KZ-1-UPB2: nedovoljena objava zasebnih pisanj;
- 143. člen KZ-1-UPB2: zloraba osebnih podatkov;
- 147. člen KZ-1-UPB2: kršitev moralnih avtorskih pravic;
- 148. člen KZ-1-UPB2: kršitev materialnih avtorskih pravic;
- 149. člen KZ-1-UPB2: kršitev avtorskim sorodnih pravic;
- 173.a člen KZ-1-UPB2: pridobivanje oseb, mlajših od petnajst let, za spolne namene;
- 176. člen KZ-1-UPB2: prikazovanje, izdelava, posest in posredovanje pornografskega gradiva;
- 211. člen KZ-1-UPB2: goljufija
- 212. člen KZ-1-UPB2: organiziranje denarnih verig in nedovoljeno prirejanje iger na srečo;
- 221. člen KZ-1-UPB2: napad na informacijski sistem;
- 235. člen KZ-1-UPB2: ponareditev ali uničenje poslovnih listin;
- 237. člen KZ-1-UPB2: zloraba informacijskega sistema;
- 247. člen KZ-1-UPB2: uporaba ponarejenega negotovinskega plačilnega sredstva;
- 248. člen KZ-1-UPB2: izdelava, pridobitev in odtujitev pripomočkov za ponarejanje;
- 251. člen KZ-1-UPB2: ponarejanje listin;
- 297. člen KZ-1-UPB2: javno spodbujanje sovraštva, nasilja ali nestrpnosti;
- 306. člen KZ-1-UPB2: izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje.

Pri pregledu uradnega prečiščenega besedila kazenskega zakonika iz leta 2012 opažamo posamezne razlike v primerjavi s Kazenskim zakonikom iz leta 2008; 173. člen je v obeh kazenskih zakonikih (KZ-1, 2008; KZ-1-UPB2, 2012) ostal nespremenjen in se glasi *spolni napad na osebo, mlajšo od petnajst let*, v zakoniku iz leta 2012 (KZ-1-UPB2, 2012) iz tega člena izhaja dodatni 173.a člen, ki se glasi: *pridobivanje oseb, mlajših od petnajst let, za spolne namene*. S členom v trenutno veljavnem zakoniku se inkriminira ne samo končni cilj storilcev (spolni napad), ampak tudi način pridobivanja oseb, mlajših od 15 let, prek komunikacijskih in informacijskih tehnologij. Poleg tega je prišlo do preimenovanja dveh členov – 237. člen (KZ-1, 2008) *vdor v poslovni informacijski sistem* je v uradno prečiščenem besedilu zakonika iz leta 2012 preimenovan v *zlorabo informacijskega sistema* (KZ-1-UPB2, 2012); 247. člen (KZ-1, 2008) *uporaba ponarejene kreditne ali druge bančne*

10 *Kazenski zakonik, ki je začel veljati 1. februarja 2008, je dodal še nekatera določila, predvsem o otroški pornografiji, s katerimi je posamezna dejanja opredelil kot kazniva (Bernik in Prislan, 2012).*

kartice pa se je preimenoval v *uporaba ponarejenega negotovinskega plačilnega sredstva* (KZ-1-UPB2, 2012).

V Sloveniji področje informacijske in kibernetske varnosti poleg Ustave in Kazenskega zakonika regulirajo tudi drugi zakoni (povzeto po Arnes, 2013): Zakon o elektronskih komunikacijah (109. člen), Zakon o varstvu potrošnikov (45.a člen), Zakon o elektronskem poslovanju na trgu (6. člen) in Zakon o varstvu osebnih podatkov (72. in 73. člen). Boj proti kibernetski kriminaliteti regulira tudi Zakon o kazenskem postopku (2012), ki opredeljuje način izvajanja predkazenskega in kazenskega postopka. Slednji v dveh členih (219.a in 223.a) ureja preiskavo elektronskih naprav ter zaseg in zavarovanje podatkov, kar je pomembno z vidika digitalne forenzike in pridobivanja digitalnih dokazov.

Čeprav ima Slovenski center za posredovanje pri omrežnih incidentih (SI-CERT) v zadnjem času več dela s preiskovanjem kibernetskih incidentov[11], je »temno polje« storilcev čedalje večje. Po besedah zaposlenih v slovenskem centru reševanje teh primerov na državni ravni že nekaj let poteka usklajeno. Težave nastanejo, ko zaradi narave interneta pride do napadov prek mednarodnega omrežja, saj so te preiskave navadno zapletene (Gabor, 2010). Po podatkih slovenske policije za obdobje 2005–2012 (Policija, 2006–2013) od leta 2005 beležimo nihanje števila kaznivih dejanj. V letu 2005 jih je bilo 52; leta 2006: 38; 2007: 113; 2008: 311; 2009: 114; 2010: 101; 2011: 276; 2012: 151. Kot je razvidno iz tabele 1, so se kazniva dejanja pretežno nanašala na napad na informacijski sistem.

Tabela 1: Število kaznivih dejanj kibernetske kriminalitete po letih (Vir: Policija, 2006–2013)

KD kibernetske kriminalitete	2005	2006	2007	2008	2009	2010	2011	2012
Zloraba osebnih podatkov	N/A	N/A	1	1	0	3	5	3
Zloraba informacijskega sistema	5	6	4	7	11	15	26	12
Kršitev materialnih avtorskih pravic	17	6	7	10	5	5	3	2
Napad na informacijski sistem	30	24	88	283	98	76	236	131
Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem	N/A	2	13	10	0	2	6	3
Skupaj	52	38	113	311	114	101	276	151

Opomba: kaznivo dejanje, v zdaj veljavnem zakoniku opisano kot »napad na informacijski sistem«, je bilo do leta 2008 opisano kot »neupravičen vstop v informacijski sistem«. Kaznivo dejanje »zloraba informacijskega sistema« se je do leta 2008 imenovalo »vdor v informacijski sistem«, v obdobju 2008–2012 pa »vdor v poslovni informacijski sistem«. N/A pomeni, da podatki o številu kaznivih dejanj niso na voljo.

Čeprav posamezna podjetja pravijo, da imajo dnevno več varnostnih incidentov (Bernik in Prislan, 2012), je število prijavljenih kaznivih dejanj relativno majhno in je v osemletnem obdobju ostalo skoraj konstantno. Neprijavljanje kibernetskih kaznivih dejanj spada med glavne težave v boju proti kibernetski

11 Iz poročila Slovenskega centra za posredovanje pri omrežnih incidentih SI-CERT (2013) je razvidno, da so v letu 2012 obravnavali več spletnih incidentov kot v letih 2010 in 2011 skupaj, in sicer 1.250.

kriminaliteti (Brenner, 2007; Wall, 2007, 2007/2010). Posamezna poročila in avtorji (AusCERT, 2005, 2006, 2010; Wall, 2007) navajajo, da je glavni vzrok, da uporabniki ne prijavljajo kibernetskih kaznivih dejanj, njihovo prepričanje, da je policija glede vloge pri zagotavljanju informacijske varnosti neučinkovita. Pojav neprijavljanja kibernetskih dejanj pa je razširjen po vsem svetu[12]. Poleg relativno majhnega števila kibernetskih kaznivih dejanj, kot je razvidno iz tabele 2, smo v Sloveniji dočakali le nekaj pravnomočnih obsodb.

Tabela 2: Število pravnomočno obsojenih polnoletnih oseb zaradi kibernetske kriminalitete po letih (Vir: Statistični urad Republike Slovenije, 2012)

KD kibernetske kriminalitete	2006	2007	2008	2009	2010	2011
Zloraba osebnih podatkov	0	0	0	2	3	6
Vdor v poslovni informacijski sistem	0	1	0	0	0	0
Kršitev materialnih avtorskih pravic	0	0	0	0	1	0
Napad na informacijski sistem	0	0	0	1	3	0
Izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem	0	0	0	0	1	0
Skupaj	0	1	0	3	8	6

Opomba: Ker so prikazani razpoložljivi podatki do leta 2011, je v tabeli uporabljeno kaznivo dejanje »vdor v poslovni informacijski sistem«, ki se je v kazenskem zakoniku iz leta 2012 preimenovalo v »zlorabo informacijskega sistema«.

Največja izrečena kazen pri vseh pravnomočnih obsodbah je šest mesecev zapora (ni prikazano) (Statistični urad RS, 2012). V obdobju od leta 2009 do 2011 je bilo največ, enajst (11), pravnomočnih obsodb izrečenih za kaznivo dejanje »zloraba osebnih podatkov«; od teh sta bili dve zaporni kazni od enega do dveh mesecev, ena zaporna kazen od dveh do treh mesecev in osem zapornih kazni od treh do šestih mesecev. Drugo največkrat obravnavano kaznivo dejanje v tem obdobju je »napad na informacijski sistem«. Od štirih pravnomočnih obsodb sta bili izrečeni dve obsodbi na zaporno kazen do dveh mesecev, dve pa na zaporno kazen od treh do šestih mesecev. Za preostala tri kazniva dejanja (vdor v poslovni informacijski sistem, kršitev materialnih avtorskih pravic na internetu ter izdelovanje in pridobivanje orožja ali pripomočkov za vdor ali napad na informacijski sistem) je bila izrečena le po ena pravnomočna obsodba. Vse tri pravnomočne obsodbe so odrejale zaporne kazni od enega do dveh mesecev.

Dobra zakonska podlaga brez organizacij, sposobnih njenega izvajanja, ni dovolj za uspešen boj proti kibernetski kriminaliteti, niti z vidika generalne prevencije (Meško, 2002). Slovenske raziskave (Bernik in Meško, 2011; Dimc in Dobovšek, 2010) ugotavljajo, da je bilo več kot 50 odstotkov anketirancev že žrtev

12 *Halder in Jaishankar (2010) sta ugotovila, da je le 9,6 odstotka indijskih spletnih uporabnikov prijavilo kibernetska kazniva dejanja. Krone in Johnson (2007) sta ugotovila, da je težave, povezane s spletnim nakupovanjem, prijavilo približno 50 odstotkov avstralskih gospodinjstev; od tega 26 odstotkov banki, 21 odstotkov drugi agenciji in tri odstotke policiji. Raziskave, ki jih je v letih 2005, 2006, 2010 opravil Australia's Computer Emergency Response Team (AusCERT), so pokazale, da avstralska podjetja redko prijavljajo kazniva dejanja (le 30- do 35-odstotno).*

kakšnega kaznivega kibernetskega dejanja[13], približno toliko anketiranih pa je takšno dejanje zagrešilo[14]. Ob upoštevanju prikazanih uradnih podatkov res lahko govorimo o velikem »temnem polju« kibernetske kriminalitete, kar je z vidika slovenske kriminalne politike zelo neugodno, po drugi strani pa omogoča odlične razmere za delovanje kibernetskih storilcev.

6 SKLEP

Kot pravi Jurij Ferme, nekdanji direktor Uprave kriminalistične policije: »Boj proti kibernetski kriminaliteti zahteva od organov pregona velike vložke, tako finančne kot kadrovske, zato je treba poiskati načine za boljšo izmenjavo specifičnih znanj, metodologij in sistemov dela organov pregona na področju preiskovanja kibernetske kriminalitete in računalniške forenzike; pri tem je pomembno tudi sodelovanje med zasebnim in javnim sektorjem.« (Uprava kriminalistične policije, 2011)

Boj proti kibernetski kriminaliteti v Sloveniji poteka na več ravneh. Center za računalniško preiskovanje pri Upravi kriminalistične policije s svojim štirimi oddelki (SKP Koper, Ljubljana, Celje in Maribor) je zadolžen za preiskavo zaseženih e-naprav oz. e-podatkov in preiskovanje kaznivih dejanj kibernetske kriminalitete. Druga nacionalna organizacija, ki kot sestavni del javnega zavoda »Arnes« deluje v preiskavi kibernetskih kaznivih dejanj, je SI-CERT, ki je velika opora pri preiskovanju kibernetske kriminalitete, ne samo zaradi strokovnosti zaposlenih, temveč tudi zaradi povezanosti s sorodnimi mednarodnimi organizacijami, kar omogoča mednarodno povezovanje in izmenjavo podatkov. Januarja 2013 je v okviru Europola začel delovati Evropski center za kibernetsko kriminaliteto. Zagotavlja boljšo operativno podporo zmogljivosti za boj proti čezmejni kriminaliteti na ravni EU, specializirane strateške ocene in ocene ogroženosti, bolj osredotočena usposabljanja ter raziskave in razvoj, ki spodbujajo razvoj posebnih orodij za boj proti kibernetski kriminaliteti. V Sloveniji so poleg državnih in mednarodnih preiskovalnih organizacij prisotna tudi zasebna informacijsko-varnostna podjetja, ki opravljajo analize in skrbijo za obvladovanje kibernetskih tveganj.

Pravna podlaga kibernetske kriminalitete je v Sloveniji del različnih nacionalnih in mednarodnih pravnih aktov, pri katerih je razvidno permanentno spreminjanje in izboljšanje. Kljub napredni pravni podlagi se v času, za katerega je značilno hitro povečevanje kibernetske kriminalitete, v Sloveniji prijavlja in obravnava malo kaznivih dejanj, še manj pa se jih konča s pravnomočno obsodbo. (Ne) učinkovitost organov pregona je predvsem odvisna od razpoložljivih finančnih sredstev. Večja državna finančna spodbuda organom pregona bi pomenila večjo tehnološko opremljenost in njeno vzdrževanje, ustrezno in permanentno usposabljanje zaposlenih in pridobivanje vodstvenih kadrov, boljšo mednarodno

13 *Bernik in Meško (2011) ugotavljata, da je bilo 57,8 odstotka slovenskih spletnih uporabnikov žrtev okužbe z virusi; skoraj 25 odstotkov jih je doživelo nadlegovanje po e-pošti. Z drugimi dejanji kibernetske kriminalitete pa se je srečalo manj kot deset odstotkov anketiranih spletnih uporabnikov.*

14 *Dimc in Dobovšek (2010) ugotavljata, da je 54 odstotkov anketiranih slovenskih spletnih uporabnikov že zagrešilo kakšno obliko kaznivega kibernetskega dejanja.*

povezavo itn. Res je, da ima slovenska Uprava kriminalistične policije posebna pooblastila v boju proti kriminaliteti, vendar se policija brez sodelovanja z drugimi nacionalnimi in mednarodnimi organizacijami in njihove pomoči ne more ustrezno boriti proti kibernetskim prestopnikom. Slovenska organizacija CERT in zasebne informacijsko-varnostne preiskovalne organizacije so lahko izjemna opora organom pregona. Poleg tega, da poročilo agencije ENISA (2012) govori o potrebi po večjem sodelovanju med organizacijami CERT in organi pregona, ni veliko dokazov o sodelovanju med Upravo kriminalistične policije in slovenskim CERT-om. Povečanje števila konkretnih dokazov o učinkovitem in zavzetem delu organov pregona bi lahko izboljšalo sodelovanje in spodbudilo uporabnike kibernetskega prostora, da bi pogosteje prijavljali kazniva dejanja. Splošno razširjeno zaupanje v delo organov pregona ni samo pokazatelj zadovoljstva javnosti z njihovim delovanjem, temveč lahko močno vpliva na povečanje učinkovitosti pravosodnih organov v boju proti kibernetski kriminaliteti.

Za boljše razumevanje kibernetske kriminalitete in njene kriminološke opredelitve imajo raziskave na tem področju pomembno vlogo. Za nadaljnje delo avtorji predlagamo podrobno preučevanje povezanosti in sodelovanja med slovenskim Centrom za računalniško preiskovanje in drugimi nacionalnimi in mednarodnimi organizacijami ter preučevanje legitimnosti organov pregona kot možen vzrok njihove (ne)učinkovitosti. Tako se bodo podrobneje izpostavile težave, s katerimi se srečujejo slovenski organi pregona, in predlagala priporočila za učinkovitejši boj proti kibernetski kriminaliteti.

LITERATURA

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M. et al. (2012). *Measuring the cost of cybercrime.* 11th Workshop on the Economics of Information Security, Berlin, Germany. Pridobljeno na http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Anonymous napadel še pedofile. (22. 10. 2011). *Žurnal24.si.* Pridobljeno na http://www.zurnal24.si/anonymous-napadel-pedofile-clanek-138518

Arnes. (2012). *Predstavitev zavoda Arnes.* Pridobljeno na http://www.arnes.si/zavod-arnes/predstavitev.html

Arnes. (2013). *Neželena elektronska sporočila (spam) in slovenska zakonodaja.* Pridobljeno na http://www.arnes.si/pomoc-uporabnikom/varnostna-priporocila/nezelena-elektronska-posta-spam/zakonodaja.html

AusCERT. (2005). *Australian 2005 computer crime and security survey*. Pridobljeno na http://www.auscert.org.au/images/ACCSS2005.pdf

AusCERT. (2006). *Australian 2006 computer crime and security survey.* Pridobljeno na *http://www.auscert.org.au/images/ACCSS2006.pdf*

AusCERT. (2010). *Australian 2010/2011 computer crime and security survey.* Pridobljeno na https://cours.etsmtl.ca/log619/documents/divers/CSIsurvey2010.pdf

Banovič, Z. (1. 7. 2007). Stopiti na prste kiber kriminalcem. *Mojmikro.si*. Pridobljeno na http://www.mojmikro.si/preziveti/varnost/stopiti_na_prste_kiber_kriminalcem

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kriminaliteto. *Revija za kriminalistiko in kriminologijo, 62*(3), 242–252.

Bernik, I. in Prislan, K. (2011). Proces upravljanja s tveganji v informacijski varnosti. V T. Pavšič Mrevlje (ur.), *Smernice sodobnega varstvoslovja: zbornik prispevkov* (str. 11). Ljubljana: Fakulteta za varnostne vede.

Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem.* Ljubljana: Fakulteta za varnostne vede.

Bogataj Jančič, M. (2008). *Avtorsko pravo v digitalni družbi.* Ljubljana: Pasadena.

Bossler, A. M. in Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management, 35*(1), 165–181.

Brenner, S. W. (2007). Private-public sector cooperation in combating cybercrime: In search of a model. *Journal of International Commercial Law and Technology, 2*(2), 58–67.

Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. *Policing: An International Journal of Police Strategies & Management, 29*(2), 408–433.

Burns, R. G., Whitworth, K. H. in Thompson, C. Y. (2004). Accessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice, 32*(5), 477–493.

Chevreau, F. R. (2006). Safety culture as a rational myth: Why developing safety culture implies engineering resilience? V E. Hollnagel in E. Rigaud (ur.), *Proceedings of the Second Resilience Engineering Symposium* (str. 63–73). Pridobljeno na http://www.resilience-engineering-association.org/download/resources/symposium/symposium-2006(2)/Chevreau_R.pdf

Council of Europe. (2013). *Convention on cybercrime: Chart of signatures and ratifications*. Pridobljeno na http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management, 35*(2), 272–284.

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(1), 240–259.

Dimc, M. in Dobovšek, B. (2010). Perception of cyber crime in Slovenia. *Varstvoslovlje, 12*(4), 378–396.

Enisa. (2011). *Slovenia country report*. Pridobljeno na http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Slovenia.pdf

Enisa. (2012). *The fight against cybercrime: Cooperation between CERTs and law enforcement agencies in the fight against cybercrime*. Pridobljeno na http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime

Eurojust. (2012). *Mission and tasks.* Pridobljeno na http://eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

Europol. (21. 1. 2013). *New European cybercrime centre (EC3) opens at Europol*. Pridobljeno na https://www.europol.europa.eu/node/1899

Gabor, M. (2010). Informacijska varnost v 2009 in kaj prinaša 2010. V *Dnevi slovenske informatike: zbornik prispevkov.* Pridobljeno na http://www.tehnokratis.si/documents/Gabor-Informacijska-varnost-v-2009.pdf

González, T. S. (2008). *Interpol's role fighting cyber crime.* Pridobljeno na http://www.nyu.edu/intercep/lapietra/Interpol_Cyber.pdf

Halder, D. in Jaishankar, K. (2010). *Cyber crime victimization in India: A baseline survey report Centre for Cyber Victim Counseling* (CCVC). Pridobljeno na http://cybervictims.org/CCVCresearchreport2010.pdf

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management, 27*(3), 341–357.

Holt, T. J., Bossler, A. M. in Fitzgerald, S. (2010). Examining state and local law enforcement perceptions of computer crime. V T. J. Holt (ur.), *Crime on-line: Correlates, causes, and context* (str. 221–46). North Carolina: Carolina Academic Press.

Huey, L., Nhan, J. in Broll, R. (2012). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice, 13*(1), 81–97.

Intervju s Tonijem Kastelicem, vodjo Centra za računalniško preiskovanje. (30. 8. 2012). *Web-center.si*. Pridobljeno na http://web-center.si/forenzika/397-intervju-z-tonijem-kastelicom-vodjo-centra-za-racunalniko-preiskovanje

Kalčina, L. (2005). *Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP) s Poslovnikom Evropskega sodišča za človekove pravice*. Ljubljana: Informacijsko dokumentacijski center Sveta Evrope pri Narodni in univerzitetni knjižnici.

Kazenski zakonik [KZ-1]. (2008). *Uradni list RS,* (55/08).

Kazenski zakonik [KZ-1-UPB2]. (2012). *Uradni list RS,* (50/12).

Krone, T. in Johnson, H. (2007). Internet purchasing: perceptions and experiences of Australian households. *Trends & Issues in Crime and Criminal Justice*, (330). Pridobljeno na http://aic.gov.au/documents/8/6/5/%7B8651CA28-C510-4B51-BA5E-EDF2F3665347%7Dtandi330.pdf

McQuade, S. (2006). Technology-enabled crime, policing and security. *Journal of Technology Studies, 32*(1), 32–42.

Meško, G. (2002). *Osnove preprečevanja kriminalitete*. Ljubljana: Visoka policijsko-varnostna šola.

Norton. (2011). *Norton cybercrime report*. Pridobljeno na http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

Norton. (2012). *Norton cybercrime report*. Pridobljeno na http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo, 60*(3), 191–198.

Policija. (2006–2013). *Letna poročila o delu policije v letih 2005–2012*. Pridobljeno na http://www.policija.si/index.php/statistika/letna-poroila

Policija. (30. 7. 2010). *Kriminalistična preiskava računalniške kriminalitete slovenske policije v sodelovanju z ameriškim FBI – informacija z novinarske konference.* Pridobljeno na http://www.policija.si/index.php/component/content/article/35-sporocila-za-javnost/8923-kriminalistina-preiskava-raunalnike-kriminalitete-slovenske-policije-v-sodelovanju-z-amerikim-fbi-informacija-z-novinarske-konference

Policija. (2012). *Twinning projekti, evropske subvencije.* Pridobljeno na http://www.mnz.gov.si/si/policija_varnost_in_nadzor/svoboda_varnost_in_pravicnost/twinning_projekti_evropske_subvencije/

Program Varnejši internet v Sloveniji: javno letno poročilo. (2012). Pridobljeno na http://www.safe.si/uploadi/editor/1369051766Centerzavarnejsiinternet-letnoporocilo.pdf

RAND Europe. (2012). *Feasibility study for a European Cybercrime Centre*: *Final report.* Pridobljeno na http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf

Prava ideja: Računalniški detektiv. (2. 2. 2010). *Rtvslo.si.* Pridobljeno na http://www.rtvslo.si/pravaideja/novica/127

Rupnik, A. (2003). *Konvencija o kibernetski kriminaliteti »Budimpeštanska konvencij*a«. Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, Slovenija, 19. in 20. maj, 2003. Pridobljeno na http://www.ltfe.org/wp-content/pdf/Kiber_kriminaliteta.pdf

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal, 17*(2), 55–71.

SI-CERT. (2013). *Poročilo o omrežni varnosti za leto 2012.* Pridobljeno na http://www.cert.si/fileadmin/slike/si-cert/fokus/2013/SI-CERT_porocilo_2012.pdf

Sommer, P. (2004). The future for the policing of cybercrime. *Computer Fraud & Security*, (1), 8–12.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassady, W. in Williams, W. P. (2001). *Electronic crime needs assessment for state and local law enforcement*. Washington: National Institute of Justice.

Statistični urad Republike Slovenije. (2012). *Polnoletni obsojenci (znani storilci) po spolu, kaznivem dejanju in glavni kazenski sankciji, Slovenija, letno.* Pridobljeno na http://pxweb.stat.si/pxweb/Dialog/varval.asp?ma=1360301S&ti=&path=../Database/Dem_soc/13_kriminaliteta/01_statistika_toz_sodisc/03_13603_obsojene_poln_osebe/&lang=2

Strniša, S. (31. 7. 2010). Vse več zlikovcev za računalniki. *Rtvslo.si.* Pridobljeno na http://www.rtvslo.si/crna-kronika/vse-vec-zlikovcev-za-racunalniki/235937

Svetek, S. in Kebe, J. (2003). Strategija računalniškega preiskovanja in analitske dejavnosti na področju kriminalitete. V M. Pagon (ur.), *Četrti slovenski dnevi varstvoslovlja: zbornik prispevko*v (str. 7). Ljubljana: Visoka policijsko – varnostna šola.

United Nations. (2000). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,* Vienna, 10-17 April 2000. Pridobljeno na http://www.uncjin.org/Documents/congr10/4r3e.pdf

Uprava kriminalistične policije. (24. 10. 2011). *Na CEPOL seminarju so o kibernetski kriminaliteti spregovorili strokovnjaki iz 15 držav.* Pridobljeno na http://www.policija.si/index.php/component/content/article/267-prispevki/60771-na-cepol-

seminarju-so-o-kibernetski-kriminaliteti-spregovorili-strokovnjaki-iz-15-drav-?lang=

Ustava Republike Slovenije. (2006). *Uradni list RS,* (68/06).

Varni na internetu. (2013). *Cilji projekta.* Pridobljeno na https://www.varninainternetu.si/cilji-projekta/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Malden: Polity.

Wall, D. S. (2007/2010). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice & Research: An International Journal, 8*(2), 183–205. Pridobljeno na http://www.google.si/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDEQFjAB&url=http%3A%2F%2Fwww.cyberdialogue.ca%2Fwp-content%2Fuploads%2F2011%2F03%2FDavid-Wall-Policing-CyberCrimes.pdf&ei=ePE2UtvmGdDHswbYx4DICw&usg=AFQjCNHtEHhy_jwjA61MUN_0OOTWC2INEg&bvm=bv.52164340,d.Yms

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*. Pridobljeno na http://fas.org/sgp/crs/terror/RL32114.pdf

Yazdanifard, R., Oyegoke, T. in Seyedi, A. P. (2011). Cyber-crimes: Challenges of the millennium age. V D. Zeng (ur.), *Advances in electrical engineering & electrical machines* (str. 527–534). Berlin: Springer.

Zakon o kazenskem postopku. (2012). *Uradni list RS*, (32/12).

O avtorjih:

Aleksandar Ilievski, magister varstvoslovja, doktorski študent na Fakulteti za varnostne vede, Univerza v Mariboru. E-mail: ilievski.aleksandar86@gmail.com

Dr. Igor Bernik, docent za informacijsko varnost, predstojnik katedre za informacijsko varnost in prodekan za izobraževalno dejavnost, Fakulteta za varnostne vede, Univerza v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si