Organizirana kriminaliteta v kibernetskem prostoru

Kaja Rus, študentka, Fakulteta za varnostne vede, Univerza v Mariboru

Namen in cilj prispevka
Namen prispevka je prikazati, da se organizirana kriminaliteta vse bolj pogosto pojavlja v kibernetskem prostoru. Nelegalne dejavnosti organizirane kriminalitete zavzemajo različna področja, zato je danes vsak posameznik lahko žrtev kibernetskega kriminala. Potrebno je izpostaviti problem in urediti sodelovanje med enotami za boj proti kibernetskemu kriminalu, saj bo boj le tako lahko uspešen.

Metoda
Osnovni pojmi so pridobljeni s preučevanjem virov in nalog, ki obravnavajo tematiko, kot jo zajema prispevek. Pri analizi rezultatov je uporabljena deskriptivna metoda, ki povzema ugotovitve avtorjev ter Komisije evropskih skupnosti, ki v svojem poročilu obravnava problem kibernetske kriminalitete. V zadnjem delu prispevka je uporabljena primerjalna metoda, saj so ugotovitve različnih avtorjev med seboj primerjane in dopolnjene z našim mnenjem.

Ugotovitve in omejitve
Omejitve se kažejo v neenotnosti definicije kibernetskega kriminala, saj različno pojmovanje le-tega pomeni neenotno zakonodajo, kar posledično pomeni nekaznovanost storilcev kaznivih dejanj. Prav tako poznamo več tipov organiziranih kriminalnih skupin, ki delujejo v kibernetskem prostoru, zato je potrebno le-te razlikovati. Organizirana kriminalita se v kibernetskem prostoru pojavlja predvsem zaradi dobička, velikega temnega polja kibernetske kriminalitete in ker je kraj storitve ter storilca kaznivega dejanja pogosto lahko zakriti ali ponarediti.

Izvirnost
Prispevek preučuje tipe organiziranih kriminalnih skupin in dejavnosti, ki jih le-te izvajajo v kibernetskem prostoru. Prav tako omenja različne možnosti za boj proti organiziranemu kriminalu v kibernetskem prostoru. Do sedaj je ta področja obravnavalo že mnogo avtorjev, a jasnih rešitev v boju zoper ta problem ni.

Ključne besede: organizirana kriminaliteta, kibernetski prostor, dobiček, nelegalna dejavnost

1. UVOD

»Danes podjetja poslujejo predvsem preko spleta, kar postaja vse bolj privlačno za vse vrste kriminalcev. Enostavne komunikacije, anonimnost in dostopnost orodij za nezakonite operacije spreminja kibernetsko kriminaliteto v globalno industrijo, ki se hitro širi in je usmerjena v dobiček, kar privlači tudi organizirano kriminaliteto« (Sani, 2011: 14).
Predstavljen je problem organizirane kriminalitete, ki se v zadnjih letih seli v kibernetski prostor. Poudarjeni sta dve vrsti organizirane kriminalitete v kibernetskem prostoru in dejavniki, ki predstavljajo resen problem v informacijski družbi. Prav tako so omenjene najbolj pogoste oblike kaznivih dejanj, ki se pojavljajo v kibernetskem prostoru. V diskusiji je predstavljeno mnenje o tem problemu, podanih pa je tudi nekaj predlogov rešitev v boju proti organizirani kriminaliteti v kibernetskemu prostoru.
Preverjeno je, da se organizirana kriminaliteta širi v kibernetskem prostoru, zato je postavljena hipoteza v obliki trditve, da je organizirana kriminaliteta prisotna v kibernetskem prostoru. Sama sem bila mnenja, da večino kaznivih dejanj v kibernetskem prostoru izvajajo hekerji, ki delujejo samostojno in ne v okviru organiziranih skupin.
Sledijo definicije osnovnih pojmov. »Organizirana kriminalna združba pomeni strukturirano skupino treh ali več oseb, ki v daljšem časovnem obdobju usklajeno deluje z namenom storitve enega ali več hudih kaznivih dejanj, da bi neposredno ali posredno pridobila finančne ali druge premoženjske

koristi« (Zakon o ratifikaciji Konvencije Združenih narodov proti mednarodnemu organiziranemu kriminalu, 2004: 1).
»Kibernetski prostor, kot imenujemo računalniško ustvarjen svet, območje informacijsko-podatkovnega prometa in vsebinsko-interesno opredeljene interakcije s pomočjo računalniško posredovanega komuniciranja v informacijska omrežja vključenih akterjev« (Trček, 1997: 19). Postaja tudi prostor, v katerem se odvija vedno večji delež družbenega delovanja in participiranja, sam dostop do računalniško generiranega prostora pa že lahko pomeni tudi ključ do oblasti in moči. Z razumevanjem te možnosti je ta prostor postal tudi področje vedno večjih konfliktov, boja za njegovo prevlado in lastništvo.
»Ker ni dogovorjene opredelitve kibernetskega kriminala, se pojmi kibernetski kriminal, računalniški kriminal, kriminal, povezan z računalniki ali kriminal visoko razvite tehnologije pogosto uporabljajo kot sopomenke. Kibernetska kriminaliteta pomeni kazniva dejanja, storjena z uporabo elektronskih komunikacijskih omrežij in informacijskih sistemov ali proti takšnim omrežjem in sistemom« (Komisija evropskih skupnosti, 2007). Kot zapišeta Bernik in Prislan (2011: 263) »zaradi splošne dostopnosti orodij in znanj so tehnike doseganja ciljev v kibernetskem prostoru postale izjemno lahke, v večini primerov primerljive z ostalo kibernetsko kriminaliteto«. V prispevku o poznavanju kibernetskih groženj in strahu pred kriminaliteto pa Bernik in Meško (2011: 243) postavita definicijo kibernetske kriminalitete, ki jo pojmujeta kot: »Kibernetska kriminalitete pomeni uporabo informacijsko komunikacijskih tehnologij za izvedbo kaznivih dejanj«.

2. REZULTATI

Komisija evropskih skupnosti (2007: 2-3), je v svojem sporočilu Komisije Evropskemu parlamentu, Svetu in Evropskemu odboru regij zapisala, da »število kibernetskih kaznivih dejanj narašča in kriminalne dejavnosti postajajo vedno bolj prefinjene in internacionalizirane, jasni kazalniki kažejo vse večjo vpletenost organiziranih hudodelskih združb v kibernetski kriminaliteto, kljub temu pa se število evropskih kazenskih pregonov na podlagi čezmejnega sodelovanja na področju kazenskega pregona ni povečalo«. Po njihovem mnenju vse večji problem predstavlja tudi nezakonito nacionalno ali mednarodno trgovanje na spletu. To vključuje trgovino z drogami, ogroženimi vrstami in orožjem.
Brennerjeva (2002) v članku »Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships«, zapiše, da do takrat še ni bilo veliko govora o organiziranem kriminalu v kibernetskem prostoru, saj je kibernetska kriminaliteta veljala za novost in niso vedeli ali se bo le-ta pojavilila tudi v kibernetskem prostoru. V tistem času so hekerji veljali za samotarje, ki se niso želeli združevati v skupine, zato njihova dejanja niso bila organizirana, saj je vsak deloval posebej. Ker pa je organizirana kriminaliteta prinaša velike dobičke v realnem svetu, je avtorica sklepala, da se bo le-ta pojavil tudi v virtualnem svetu.
Choo in Smith (2008), v prispevku govorita o dveh tipih organiziranih kriminalnih skupin. Prvi tip predstavljajo tradicionalno organizirane kriminalne skupine, ki so hitro ugotovile povezavo med pomembnimi informacijami in komunikacijskimi tehnologijami za povečanje ali izboljšanje njihovih kriminalnih dejavnosti. Informacijsko komunikacijsko tehnologijo uporabljajo za olajšanje trgovanja z drugo, poslovnimi skrivnostmi, prav tako jim pomagajo pri izsiljevanju, pranju denarja in distribuciji nelegalnih materialov. Povezanost med tradicionalno organiziranimi kriminalnimi skupinami in informacijsko komunikacijsko tehnologijo se povečuje in postaja vse bolj pomemben.
Drugi tip predstavljajo organizirani kibernetski kriminalci, ki jih »sestavljajo posamezniki, ki si delijo podobno mnenje in se po običajno poznajo le preko spleta, a organizirano sodelujejo pri dosegu skupnega cilja« (Choo in Smith, 2008: 40). Tovrstne skupine si navadno želijo finančnega dobička, včasih pa imajo tudi druge cilje. Večinoma so ohlapno strukturirane in fleksibilne. Choo in Smith sta tudi poudarila, da je za ljudi, ki se ukvarjajo z kriminalom preko informacijske tehnologije veliko lažje, saj ne vidijo svojih žrtev in tako »ne čutijo svoje roke v tujem žepu« (Choo in Smith, 2008: 40).
»Dejavniki, zaradi katerih predstavlja kibernetski kriminal resen problem v informacijski družbi, so (Bogataj Jančič, Klemenčič, Makarovič, Tičar in Toplišek, 2007: 331):

- Prav ti dejavniki, ki kažejo na resen problem kibernetske kriminalitete, pa delujejo kot nekakšna zaščitna odeja za organizirano kriminaliteto, kot so velika ekonomska in družbena škoda;

- Narava računalniških komunikacij, kjer državne meje ne predstavljajo ovir pri pretoku informacij, storilci pa se pogosto ne nahajajo v isti državi;
- Tehnične ranljivosti informacijskih sistemov;
- Slaba tehnična opremljenost in usposobljenost organov odkrivanja in pregona, ki ne more dohajati hitrega napredka tehnologije;
- Togost in počasnost pravnega urejanja področja kibernetske kriminalitete;
- Ovire pri mednarodnem sodelovanju organov pregona, ki so pogojene s klasičnimi pravicami suverenih držav oz. pravnih sistemov;
- Veliko temno polje kibernetske kriminalitete;
- Identiteto storilca in izvirni kraj storitve dejanje je mogoče razmeroma preprosto zakriti ali ponarediti, kar otežuje njihovo izsledite v«.

Vsak dejavnik vpliva na zaščito organizirane kriminalitete pred odkritjem, saj so to največje prednosti, ki jih organizirana kriminaliteta vidi v kibernetskem prostoru za nemoteno nadaljevanje njihovih poslov. Bernik in Meško (2011: 249) sta v svoji študiji poznavanja kibernetskih groženj in strahu pred kriminaliteto ugotovila, da se manj kot polovica ljudi zaveda, da je lahko »žrtev kibernetske kriminalitete vsakdo, ki uporablja računalnik. To nakazuje na majhno ozaveščenost, po drugi strani pa tudi dejstvo, da se z računalnikom v zasebnem prostoru, stran od javnosti, mnogi počutijo varne in se jim zdi, da kibernetski prostor nima stika z realnostjo in je ločen od realnega dogajanja«. Avtorja ugotavljata, da se »mnogo ljudi boji uporabiti kreditno kartico v spletni trgovini, kljub majhnemu številu tovrstnih zlorab. To pa potrjuje dejstvo, da medijsko odmevni primeri vzpodbudijo višjo stopnjo strahu, kot pa je dejanska možnost za viktimizacijo« (Bernik in Meško, 2011: 242). Menim, da se problem organizirane kriminalitete v kibernetskem prostoru v medijih ne pojavlja tako pogosto, kar pa vpliva na nizko stopnjo ozaveščenosti ljudi in posledično na slabše odkrivanje in neuspešen boj proti organiziranim kriminalnim skupinam v kibernetskem prostoru.

Nelegalne dejavnosti organizirane kriminalitete v kibernetskem prostoru (vzeto po Choo in Smith, 2008: 44-47) so:

1. Plačila preko interneta omogočajo »premikanje večjih vsot denarja preko različnih pristojnosti, kar omogočajo goljufije in pranje denarja«. Dobovšek (2009: 5) v svojem prispevku pojmuje pranje denarja kot »vsako tehniko pretvarjanja nepošteno in nezakonito pridobljenega bogastva v pošten in zakonit prihodek. Primarni cilj pranja denarja je prikrivanje nezakonito pridobljenega dohodka in izmikanje odkrivanju kriminalnih finančnih malverzacij ter s tem izogibanje plačila davščin. Denar postane s tem, ko je opran, del legalnega plačilnega prometa«.
2. Dražbe preko interneta »za kupce in prodajalce ustvarjajo globalni in virtualni trg, kjer lahko prodajajo ali kupujejo s pomočjo konkurenčnih ponudb«. To pa omogoča organiziranim kriminalnim skupinam, da vplivajo na nakup in na ceno nakupa ter ob enem perejo denar. To storijo tako da, postavijo na dražbo predmet, katerega vrednost je precenjena ali podcenjena. Ko se licitacija konča, kupec plača z nezakonito pridobljenim donosom, prodajalca pa izvor tega denarja ne zanima. Ko je plačilo končano, lahko investirajo čiste dohodke v legalne dejavnosti.
3. Igre preko interneta so rastoča industrija, ki omogočajo igralcem, da tekmujejo med seboj v virtualno ustvarjenih svetovih. »Da pa se v tovrstne igre sploh lahko vključijo, morajo igralci najprej plačati določen znesek, kar jim omogoča nakup virtualne valute, virtualno nastanitev, virtualno blago itd.«. Ker opravijo plačilo preko interneta, lahko organizirane kriminalne skupine uporabijo njihove osebne podatke za krajo identitete ali pa za izsiljevanje. Prav tako lahko igralcem prodajajo neobstoječe elemente v igri, priredijo programsko opremo v svoj prid, tako da so lahko le oni zmagovalci iger, kjer se dobi denarno nagrado, razširjajo spyware preko elektronske pošte, pedofilija pri virtualno ustvarjenih otrocih in podobno.
4. Socialne spletne strani kot so Friendster, MySpace in Facebook omogočajo uporabnikom, da objavijo svoje osebne podatke in fotografije, ki pa jih lahko vidijo tudi tretje osebe, zato obstaja možnost za krajo identitete.

»Namen vseh teh dejavnosti je ustvarjanje dobička, ki pa se s pranjem denarja kot sekundarno dejavnostjo preliva v legalne finančne tokove. Za organizirano kriminaliteto so značilni visoka profesionalnost, organiziranost in skorajda neomejena finančna sredstva, zato se razmere na tem

področju nenehno zaostrujejo. Dobički predstavljajo naraščajočo nevarnost za državo in družbo, saj jih z ene strani investirajo v povsem legalne posle (pranje denarja), z druge strani pa predstavljajo velikanski korupcijski potencial« (Dobovšek, 2009: 5).
Organizirana kriminaliteta v kibernetskem prostoru torej predstavlja vse večjo grožnjo sodobnemu delovanju in izmenjavanju podatkov v kibernetskem prostoru.

3. RAZPRAVA

Kibernetska kriminaliteta predstavlja vse večje težave v današnjem svetu. To je potrdila tudi Komisija evropskih skupnosti (2007: 3), ki je v svojem Sporočilu komisije Evropskemu parlamentu, Svetu in Evropskemu odboru regij zapisala, da je »varstvo posameznikov proti kibernetski kriminaliteti pogosto oslabljeno zaradi vprašanja določanja ustrezne sodne pristojnosti, prava, ki se uporablja, čezmejnega kazenskega pregona ali priznanja uporabe elektronskih dokazov«. Prav ta vprašanja pa omogočajo organizirani kriminaliteti uporabo kibernetskega prostora za izvajanje kaznivih dejanj.
V analizi rezultatov so vsi avtorji potrdili hipotezo, da je organizirana kriminaliteta prisotna v kibernetskem prostoru in to v veliki meri. Po pregledu literature ugotavljam, da organizirane kriminalne skupine uporabljajo različne dejavnosti za pridobivanje finančnih koristi in vse te dejavnosti so v današnjem času tako pogoste, da je lahko posledično skoraj vsak žrtev organizirane kriminalitete prek spleta. Zupančičeva (2005) zapiše, da je kazniva dejanja v kibernetskem prostoru težko odkriti, zato pogosto ostajajo neopažena ali pa celo nekaznovana. Prav ta dva dejavnika neodkritost in nekaznovanost ščitita organizirano kriminaliteto pred organi kazenskega pregona.
Kaj pa lahko storimo za boj proti organizirani kriminaliteti v kibernetskemu prostoru? Kot prvo, je potrebno ozaveščati ljudi o nevarnostih, ki pretijo na spletu. Pred pripravo prispevka, se nisem zavedala, da tudi organizirane skupine izkoriščajo dejavnosti, ki jih opravljamo preko interneta. Menila sem, da so to večinoma samostojni hekerji, ki želijo priti do finančnih koristi.
Druga stvar, ki jo moramo urediti za uspešen boj proti organizirani kriminaliteti na spletu je, »z usklajevanjem razviti politični okvir EU o boju proti kibernetski kriminaliteti, skupaj z državami članicami, zadevnimi organizacijami EU in mednarodnimi organizacijami ter drugimi interesnimi skupinami« (Komisija evropskih skupnosti, 2007: 4). Posledično je potrebno med državami uskladiti zakonodajo na področju kibernetske kriminalitete, saj je učinkovito sodelovanje med organi kazenskega pregona odvisno od obstoja vsaj delno usklajenih opredelitev kaznivih dejanj.
Kot najpomembenjši dejavnik za izboljšanje boja proti organizirani kriminaliteti pa je ureditev in olajšanje usklajevanja in sodelovanja med enotami za boj proti kibernetski kriminaliteti, drugimi zadevnimi organi in strokovnjaki v EU. Ker organizirana kriminaliteta pogosto presega državne meje, je za uspešen boj zelo pomembno mednarodno sodelovanje organov kazenskega pregona, saj lahko le z uspešnim sodelovanjem dosežemo želeni cilj, torej zmanjšanje organizirane kriminalitete v kibernetskem prostoru.
Dejavnikov, zaradi katerih predstavlja kibernetska kriminaliteta resen problem v informacijski družbi, ne moremo preprosto izničiti, lahko pa se borimo proti večanju kibernetske kriminalitete in organizirane kriminalitete v njej. Odkrivanje le tega sicer ni preprosto, zato je potrebno sprejeti določeno zakonodajo, ozavestiti ljudi o tem problemu, predvsem pa urediti pogoje za nemoteno delovanje in sodelovanje organov kazenskega pregona, saj bomo le tako lahko preprečili širjenje organizirane kriminalitete v kibernetskem prostoru.

VIRI

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). Informacijsko bojevanje v Sloveniji – od tradicionalno lokalnega v globalni kibernetski prostor. Varstvoslovje, 13(3), 261-279.

Bogataj Jančič, M., Klemenčič, G., Makarovič, B., Tičar, K. in Toplišek, J. (2007). Pravni vodnik po internetu. Ljubljana, GV Založba.

Brenner, S.W. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. North Carolina Journal of Law&Technology, 4(1), 1-50.

Choo, K.R. in Smith, R.G. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups. Asian Criminology, 3, 37-59.

Dobovšek, B. (2009). Sodobna ogrožanja, kako odvrniti nevarnosti?. Pridobljeno 16. decembra 2011, http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/2005/PDF/CIP/02_06_09_SEMINAR-dr.DOBOVSEK.pdf

Komisija evropskih skupnosti. (2007). Delovni dokument služb Komisije - Spremni dokument k sporočilo Komisije Evropskemu parlamentu, Svetu in Evropskemu odboru regij - Na poti k splošni politiki o boju proti kibernetskemu kriminalu. Pridobljeno 4. decembra 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007SC0641:SL:NOT

Sani, R. (2011). Cyber crime-buster to the fore. New Straits Times. Jun 27, 14.

Trček, F. (1997). Dostopnost in izključenost v kiberprostoru: računalniško posredovano komuniciranje in spremembe prostorsko-časovne organizacije. Magistrska naloga, Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.

Zakon o ratifikaciji Konvencije Združenih narodov proti mednarodnemu organiziranemu kriminalu. (2004). Uradni list RS, št. 41/2004.

Zupančič, T. (2005). Zaznavanje deviantnega vedenja na internetu med mladimi. Diplomsko delo, Ljubljana: Fakulteta za družbene vede.