STRUČNI RAD – PROFESSIONAL PAPER 10.7251/ZRPIM2101443D

KRIMINOLOŠKI ASPEKTI INTERNETA I NJEGOVA ULOGA U *CYBER* KRIMINALU

Biljana Dimitrić

Univerzitet PIM, Pravni fakultet, Despota Stefana Lazarevića bb, 78 000 Banja Luka, Bosna i Hercegovina, biljanazdimitric@gmail.com

SAŽETAK

Zbog mnogih karakteristika, Internet zaslužuje posebnu pažnju u kriminologiji, kao i krivičnom pravu i politici. Internet je danas postao globalni, trenutni, interaktivani modul i civilizacijski aparat koji omogućava automatizovanu obradu informacija. Zbog raznovrsnih karakteristika, internet pruža jedinstvene mogućnosti za sajber kriminal, što uključuje upotrebu računarskih mreža za ostvarivanje tog cilja. Ovaj rad nudi jedan pregled istraživanja o tome kako i zašto Internet pruža jedinstvene mogućnosti za kriminalne aktivnosti, kao i šta ovo znači za upravljanje (sajber) kriminalom odnosno visokotehnološkim kriminalom. Skicira neke tipologije sajber kriminala i navodi određene faktore rizika na Internetu koji, kada se kombinuju, stvaraju specifični podsticajni okvir za kriminal. Sam rad se ukratko bavi prijetnjama i ranjivostima sprovođenja zakona i drugih protivmjera, kao i onim što se malo zna o sajber kriminalcima, organizovanom kibernetičkom kriminalu i sajber žrtvama. Uprkos oskudnosti empirijskih studija o kibernetičkom kriminalu, odnosno sajber kriminalu, teorijski nalazi i hipoteze izneseni u literaturi potkrepljuju zaključak da Internet mijenja kriminal i da se stvara jedna nova vrsta adaptibilnosti. Istraživaja ukazuju da kibernetički kriminal postaje sve organizovaniji, obimniji i raznovrsniji, sa sve većom podjelom rada i da je sve više u sinergiji sa takozvanim oflajn organizovanim kriminalom. Štaviše, čini se da kod određenih krivičnih djela postoji velika korelacija između viktimizacije van mreže i na mreži. Sada kada je upotreba Interneta postala uobičajena pojava u svakodnevnom životu, kriminologija, kao i krivično pravo i politika, trebalo bi da češće uključuju Internet i sajber kriminal u svoju svakodnevnu praksu, istovremeno još više fokusirajući pažnju na osobenosti i nijanse Interneta kao posebnog fenomena.

Ključne riječi: kriminologija, pravo, internet, sajber criminal.

UVOD

Internet, kao globalni fenomen razvijen 1960-ih godina dvadesetog vijeka, tek sredinom 1990-ih postaje veliko prodajno mjesto za široku populaciju, tako da je samim tim privukao i interes vlada i kriminologa. Ranije je akcenat bio na računarskom oflajn kriminalu, međutim sada je u prvi plan izašao sajber kriminal, a samim tim naglašavajući činjenicu da su računarske mreže - ili „sajber prostor“ - postavile nove pravne i političke izazove (Chang, & Grabosky, 2014; Rajput, 2020). Zbog mnogih svojih karakteristika i mogućnosti manipulacije, Internet treba posebno razmotriti kao plodno tlo za razne protivzakonske aktivnosti. Internet, kao globalna platforma, omogućava ljudima da komuniciraju u realnom vremenu bez obzira na njihovo mjesto stanovanja. Kao rezultat svega toga, vrijeme, udaljenost i granice igraju mnogo manju ulogu u visokotehnološkom nego u konvencionalnom kriminalu. Budući da je Internet digitalna mreža, on omogućava automatizovani prenos podataka i informacija velikom brzinom u masovnim proporcijama i razmjerama (Lin, & Nomikos, 2018; Mowery, 2013). Visokotehnološki kriminal je okarakterisan kao vrsta krivičnog djela u kome se računarske mreže koriste kao "meta" ili kao "oružje". Zbog neobične prirode Interneta, sajber kriminal zaslužuje posebno razmatranje sa kriminološkog stanovišta (Luong, 2019).

Tipologija

Ko su hakeri? Hakeri su osobe koje traže i koriste nedostatke u računarskim sistemima ili mrežama kako bi im pristupile. Oni su obično iskusni računarski programeri koji se dobro razumiju u računarsku sigurnost (Kranenbarg, Ruiter, Gelder, & Bernasco, 2018). Da bi se shvatio na pravi način visokotehnološki kriminal potrebno je napraviti određene distinkcije, jer se motivi i metode prestupnika mogu razlikovati u zavisnosti od oblika sajber kriminala. Razlika između Interneta kao alata i Interneta kao cilja je najpopularnija. Evropska komisija 2007. opisuje kibernetički kriminal, odnosno visokotehnološki kriminal, kao „krivična djela počinjena korišćenjem elektronskih komunikacionih mreža i informacionih sistema". Pored računarskih mreža kao sredstva izvršenja ili predmeta zločina, Donn Parker (1983) je identifikovao i treću kategoriju u kojoj računari služe kao mjesto zločina, u smislu pružanja manje ili više neutralne pozadine zločina (Parker, 1983). Tipologija Interneta kao entiteta, alata ili okruženja ogleda se u možda najkorisnijoj kategorizaciji sajber kriminala koja se danas koristi – listi teških krivičnih djela Savjeta Evrope (Buono, 2012):

Nezakonit pristup (hakovanje), ilegalno presretanje, ometanje podataka (npr. virusi), ometanje sistema (npr. napadi uskraćivanja usluge) i zloupotreba aplikacija (npr. posjedovanje hakerskog softvera) – svi su primjeri različitih elemenata krivičnih djela protiv bezbjednosti, integriteta i dostupnosti računarskih podataka i sistema.

Zločini povezani sa računarom, poput falsifikovanja i prevare;

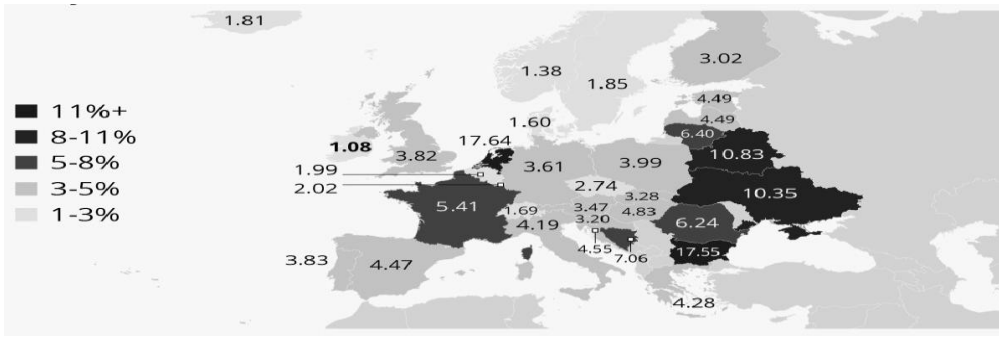
Krivična djela u vezi sa sadržajem i autorskim pravima; prvi uključuje dječiju pornografiju (rasizam je obuhvaćen posebnim protokolom uz Konvenciju).

Wall predlaže novu, hronološku tipologiju, zasnovanu na promjenljivoj podsticajnoj strukturi sajber kriminala (Wall, 2004; Wall, 2003; 2007). Tradicionalni zločini u kojima su (samostalni) računari samo sredstvo izvrsenja čine prvi talas sajber kriminala; oni se nazivaju sajber kriminalom „niskog nivoa". Od 1970-ih nadalje, drugu generaciju čine zločini koje omogućavaju lokalne ili globalne računarske mreže; to su često konvencionalni zločini, ali oni stvaraju nove globalizovane mogućnosti i pitanja jurisdikcije. Treća generacija se sastoji od „stvarnih zločina u potpunosti posredovanih tehnologijom", koji predstavljaju „korak u evoluciji sajber kriminala" (Wall, 2013).

Hakeri i sajber kriminal

Hakovanje se obično smatra krivičnim djelom, osim ako korporacija naredi hakeru da testira njihov sistem uz izričito odobrenje. Ovo testiranje je opravdano, jer je žrtvi neovlašćenog pristupa podacima nemoguće utvrditi šta je haker uradio i zašto, a bezbjednost računarskog sistema je ugrožena (Levi, 2017). Takođe zato što su etablirane institucije sajber prostora iskoristile moć konceptualne šeme u svojoj potrazi za redom i kontrolom. Hakovanje je postalo „prožeto normativnim značenjem čije se jezgro odnosi na štetna i preteća djela i kao rezultat toga je praktično nemoguće govoriti, a kamoli identifikovati hakere koji se bave aktivnostima značajne društvene hrabrosti." (Grabosky, & Walkley, 2007). Međutim, porijeklo subkultura u hakerskoj zajednici je variralo, neki su bili samo znatiželjni ljudi, drugi su bili „utopisti", a neki su bili snažno anti-establišment anarhistički orijentisani tako da su u popularnoj kulturi dobili naziv „cyberpunk". Potonje grupe ili pojedinci bili su (i još uvijek su) voljni da oštete velike sisteme informacija, ako bi im to pomoglo da postignu svoje ciljeve, što ih čini destruktivnim entitetima u društvu. Štaviše, kako je Internet postajao sve dostupniji tokom 1990-ih, druge razne organizacije počele su da koriste hakovanje iz drugih razloga, kao što su finansijska dobit, ekstremizam i drugi oblici „haktivizma" (Lu, Liang, & Taylor, 2010; Lusthaus, 2012). Istraživanja na polju visokotehnološkog kriminala ukazuju da ne postoji samo jedna vrsta sajber kriminalaca. Jedna od činjenica koja se uviđa tokom istraživanja visokotehnološkog kriminala je da su sajber "kriminalci" uglavnom mladi, sa određenim poteškoćama u socijalnoj interakciji i pate od raznih mentalnih bolesti (anksioznost, depresija) i poremećaja ličnosti (narcisoidnost, psihopatija) i invaliditeta. Iako nesumnjivo ima onih koji ne spadaju u ovu kategoriju, opet postoji širok spektar ljudi koji se bave sajber-kriminalom (Norris, Brookes, & Dowell, 2019). Prema istraživanjima većina onih koji su učestvovali u Dark Marketu, globalnom sajtu za trgovinu sajber kriminalom, bili su između 17 i 40 godina starosti (Reyns, & Henson, 2016). Dalje, postoje značajne razlike između hakerskih podgrupa, a stereotipni haker je daleko od običnog "kriminalca" kakve ih poznajemo kroz istoriju i kakve ih viđamo preko dostupnih medija. Neke karakteristike izvršioca sajber kriminala mogu se

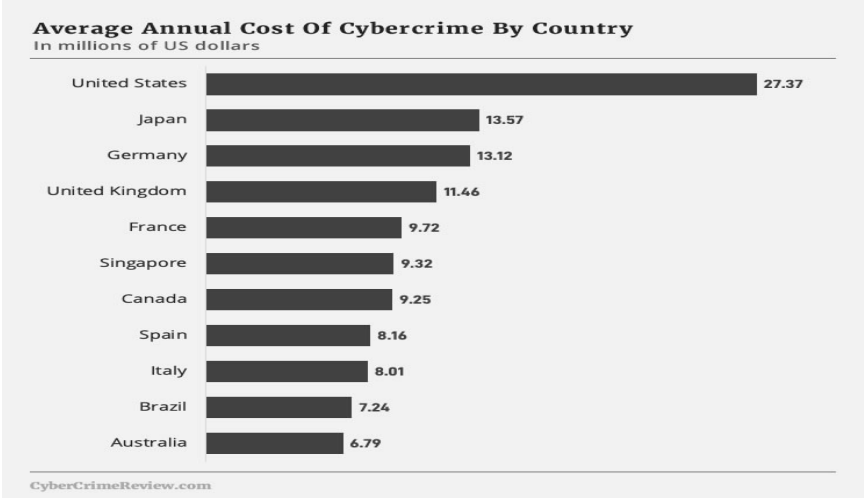
identifikovati, ali treba napomenuti da je, kao i kod podataka o rasprostranjenosti, dostupno malo empirijskih dokaza o prestupnicima (sa izuzetkom nekoliko jedinstvenih kategorija, kao što su „sajberstalkers" i dječji pornografi) (Oddis, 2002; Srivastava, Das, Udo, & Bagchi, 2020).



Slika 1. Zemlje Evrope: Napadi sajber kriminalaca izraženi u procentima (Statissta, 2019).
Figure 1. Country of Europe: Cybercrime attacks expressed as a percentage (Statissta, 2019).

Pravna vizura sajber kriminala

Kriminalizacija nepoželjnog ponašanja na mreži ima dva efekta: stvara pravni presedan za retributivnu represiju nad tim ponašanjem i stvara okruženje društvene neprihvatljivosti kibernetičkog kriminala, osporavajuci i stigmatizujući takvo ponašanje. Mnogi koji koriste internet za vršenje zločina odrasli su i družili su se u okruženju u kojem je stvarni kriminal u različitim oblicima bio dominantan način nezakonitog ponašanja (Martin, & Rice, 2011). Kašnjenje u donošenju krivičnog zakonodavstva početna je prepreka za pravne strukture. Tradicionalni krivični zakoni ciljaju fizičke predmete, dok visokotehnološki kriminal cilja nematerijalne predmete poput znanja i informacione tehnologije (Cordova, Álvarez, Ferrandiz, & Pérez-Bravo, 2018). Na primjer, bankovne račune široko koriste pojedinci, preduzeća i organizacije, a stanjem na ovim računima upravlja se putem Interneta i elektronskih usluga. Hakeri mogu ciljati račune kako bi ukrali cjelokupna ili dio sredstava. Ovo nije fizički predmet, jer dok se fizički novac skladišti u trezorima banke ono što se zapravo krade, kada se taj novac krade hakovanjem, su digitalne informacije, a stanje sa računa ilegalno se prenosi na drugi. Neki stručnjaci klasifikuju virtuelnu imovinu kao elektronsku valutu (npr. BitCoin), definisanu kao „vrijednost koja se elektronski čuva u sistemu, kao što je čip kartica ili hard disk u personalnom računaru" (Kleijssen, & Perri, 2017; Veresha, 2018). Štaviše, pošto su izvršioci možda hiljadama kilometara udaljeni od mjesta na kojem se javljaju simptomi, identifikacija kibernetičkog kriminala u nekim situacijama može biti teška. Izveštaji žrtava o visokotehnološkom kriminalu mogu ukazivati na problem sa otkrivanjem sajber kriminala, posebno ako su žrtve preduzeća. Ovo stanje može biti objašnjeno sledećim faktorima: postupak gonjenja može štetiti poslovanju žrtve, nanoseći štetu čak i kada pokušava da ga riješi; postoji rizik od otkrivanja osjetljivih informacija; čak i ako se zločin dokaže, zakon ne garantuje nadoknadu pretrpljene štete (Gercke, 2008).



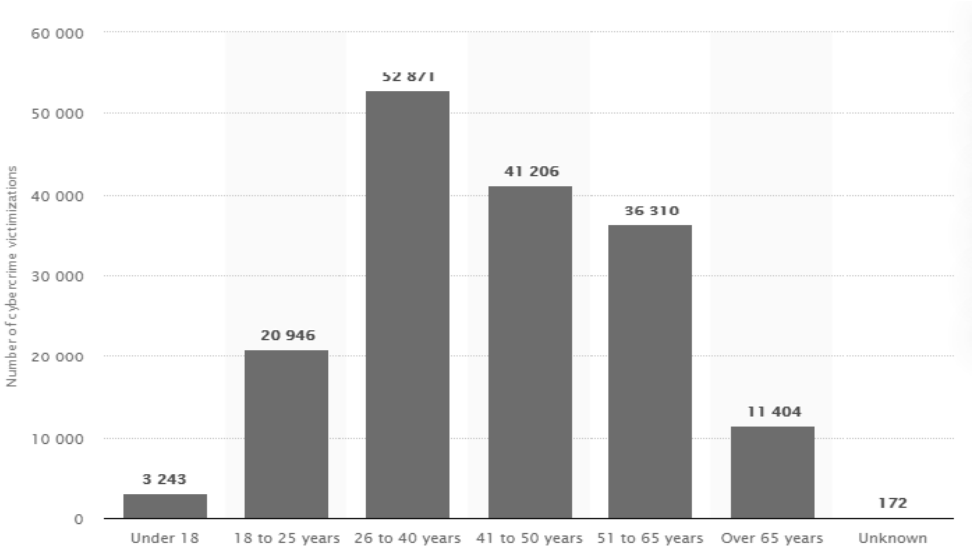
Slika 2. Prosječni godišnji gubici zbog sajber kriminala (Cyber Crime Reiview, 2021).
Figure 2. Average annual losses due to cybercrime (Cyber Crime Reiview, 2021).

Spam kao jedan od najčešćih internet zloupotreba se opisuje kao prenos neželjenih masovnih poruka. Iako regulacija neželjene pošte nije obuhvaćena međunarodnim ugovorom, rizici širenja malvera i krađe identiteta podstakli su neke regionalne pravne instrumente da pokušaju da smanje ovu praksu kako bi smanjili svoje negativne posljedice. Prema drugom kriterijumu za krivična djela sajber kriminala jedan od najčešćih oblika sajber kriminala je krađa identiteta, u kojoj izvršioci koriste Internet za krađu ličnih podataka od drugih korisnika (Wall, 2012). Korisnicima se preporučuje da koriste stranice koje se čine legitimnim, ali u stvarnosti su lažne, tražeći lične informacije, poput podataka za prijavu, sastavljene od uvođenja korisničkog imena i lozinke, telefonskih brojeva, brojeva kreditnih kartica, brojeva bankovnih računa. Dakle, ove informacije kriminalci mogu koristiti za krađu „identiteta“ druge osobe (Montoya, Junger, & Hartel, 2013).

Sajber žrtve

Istraživanja, koja su obuhvatila populaciju starosti od 15 do 75 godina, ukazuju da su, pored starosti, i drugi faktori kao što su obrazovanje i ekonomski status povezani sa žrtvom sajber kriminala. Prethodne studije pokazale su da su mladi i visokoobrazovani korisnici socijalno više angažovani i stoga imaju veću verovatnoću da isprobaju nove mrežne usluge i proizvode (Whitty, 2019). To može na određene načine povećati vjerovatnoću da postanete žrtva sajber kriminala, ali tačna logika da postanete žrtva sajber kriminala ostaje nepoznata. Rezultati istraživanja, takođe, sugerišu da bi se buduća istraživanja trebala usredsrediti na šire društveno-ekonomske faktore koji bi mogli uticati na sajber kriminal. Čak i više nego kod sajber kriminalaca, sajber žrtve su nepoznata grupa. Ankete o viktimizaciji daju neke podatke o prevalenciji, ali je malo podataka dostupno o faktorima rizika za određene grupe žrtava (Rokven, Boer, Tolsma, & Ruiter, 2017). Ankete među organizacijama sugerišu da preduzeća i javne agencije znatno pate od sajber kriminala. Podaci se, međutim, veoma razlikuju. U 2002. Američko istraživanje Instituta za računarsku sigurnost i FBI utvrdili su da je 90% organizacija prijavilo kršenje bezbjednosti računara u prethodnoj godini, od njih 80% prijavilo je finansijski gubitak kao rezultat; dok je globalno istraživanje rađeno 2000. godine u 12 zemalja od strane KPMG, došlo do podatka da je samo 9% organizacija prijavilo kršenje sigurnosti u prethodnoj godini (Holt, & Bossler, 2013). Čini se da je razlika prevelika da bi se objasnila nacionalnim razlikama ili dvogodišnjom razlikom u mjerenju. Nekoliko drugih istraživanja izvještava o incidencijama od 10% do 40% viktimizacije organizacije. Sve u svemu, nalazi sugerišu da je kibernetički kriminal stvaran problem, ali da nije rašireniji od ostalih vrsta kriminala. Tokom poslednje tri godine, 5,3 procenata ispitanika starosti od 15 do 24 godine izjavilo je da su postali žrtve sajber kriminala (Caneppele, & Aebi, 2019; Holt, Wilsem, Weijer, & Leukfeldt, 2020). U najgorem slučaju, kibernetički kriminal potencijalno može

izazvati ljudima toliko strepnje kao bilo koji drugi ozbiljni zločin. Određene studije otkrivaju da je postajanje žrtvom sajber kriminala povezano sa nasilnim interakcijama van mreže, kao i drugim potencijalnim psihosocijalnim problemima, ističući potrebu za daljim istraživanjima (Casey, & Nikkel, 2020). Kao primjer navodimo starost žrtvi koje su bile meta sajber "kriminalaca" u Španiji 2019. godine.



Slika 3. Starost žrtvi koje su bile meta visokotehnološkog kriminala (Statissta, 2021).
Figure 3. Age of victims who were the target of high-tech crime (Statissta, 2021).

ZAKLJUČCI

Zahvaljujući različitim karakteristikama, Internet nudi raznovrsne mogućnosti za brojne kriminalne radnje. Mnoge od ovih karakteristika čine Internet onim po čemu je poznat: ogromna, globalna, pristupačna mreža koja omogućava trenutne komunikacije i koja je promijenila društvene i ekonomske procese. Takođe se očekuje da transformiše i kriminal, s obzirom na njegov efekat u informatičko doba. U literaturi je identifikovano desetak faktora rizika koji doprinose specifičnoj strukturi prilika za kibernetički kriminal: globalni opseg, deteritorijalizacija, svestrana mrežna struktura, privatnost, daljinski kontakt sa prekršiocima, manipulacija podacima, automatizacija zločina, velika veličina, agregacija manjih šteta. Otprilike u isto vrijeme, podsticajni okvir Interneta za sajber kriminal predstavlja prijetnju istraživanju i politici upravljanja Internetom. Ne videći potencijalne sajber "kriminalce" iza svake IP adrese, budućnost Interneta već je ispunjena preprekama za višestepeno i policentrično upravljanje, ali korišćenje Interneta ne može i dalje ignorisati brojne mogućnosti za zločin na toj platformi i rizike od viktimizacije. U ovom radu nisu detaljno obrađene teme sajberbulinga, tako da je sa te strane rad ostao limitiran. Kriminolozi, pravnici i istraživači Interneta trebalo bi da sarađuju kako bi razvili sistemske pristupe regulativi Interneta koji minimiziraju kriminalne ranjivosti, zadržavajući što više jedinstvenog karaktera Interneta.

LITERATURA

Buono, L. (2012). Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3). *New Journal of European Criminal Law*, *3*(3–4), 332–343.

Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, *13*(1), 66-79.

Casey, E., & Nikkel, B. (2020). Forensic analysis as iterative learning. *The Security of Critical Infrastructures*, 177.

Cyber Crime Reiview. (2021). Report. Retrieved May 15, 2021, from http://cybercrimereiview.com/

Chang, L. Y., & Grabosky, P. (2014). Cybercrime and establishing a secure cyberworld. *In The Handbook of Security* (pp. 321-339). Palgrave Macmillan, London.

Cordova, J. G. L., Álvarez, P. F. C., Ferrandiz, F. de J. E., & Pérez-Bravo, J. C. (2018). Law versus Cybercrime. *Global Jurist*, *18*(1).

Gercke, M. (2008). National, Regional and International Legal Approaches in the Fight Against Cybercrime. *Computer Law Review International*, *9*(1), 7–13.

Grabosky, P., & Walkley, S. (2007). Computer crime and white-collar crime. In *International handbook of white-collar and corporate crime* (pp. 358-375). Springer, Boston, MA.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, *38*(2), 187-206.

Kleijssen, J., & Perri, P. (2017). Cybercrime, evidence and territoriality: Issues and options. *In Netherlands Yearbook of International Law 2016* (pp. 147-173). TMC Asser Press, The Hague.

Kranenbarg, M. W., Ruiter, S., Gelder, J.-L. van, & Bernasco, W. (2018). Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison. *Journal of Developmental and Life-Course Criminology*.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

Lin, L. S., & Nomikos, J. (2018). Cybercrime in East and Southeast Asia: The Case of Taiwan. *In Asia-Pacific Security Challenges* (pp. 65-84). Springer, Cham.

Lu, H., Liang, B., & Taylor, M. (2010). A comparative analysis of cybercrimes and governmental law enforcement in China and the United States. *Asian journal of criminology*, *5*(2), 123-135.

Luong, H. (2019). Cybercrime in Legislative Perspectives: A Comparative Analysis between the Budapest Convention and Vietnam Regulations. *International Journal of Advanced Research in Computer Science*, *10*(3).

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*, *13*(2), 71-94.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803–814.

Montoya, L., Junger, M., & Hartel, P. (2013, August). How" Digital" is Traditional Crime? *In Proceedings 2013 European Intelligence and Security Informatics Conference* (pp. 31-37). IEEE.

Mowery, S. P. (2013). *Defining Cyber and Focusing the Military's Role in Cyberspace*. Army war College Carlisle Barracks Pa.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Oddis, D. I. (2002). Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime. *Temple International & Comparative Law Journal*, *16*, 477.

Parker, D. B. (1983). *Fighting Computer Crime*. Scribner.

Rajput, B. (2020). Exploring the Phenomenon of Cyber Economic Crime. *In Cyber Economic Crime in India* (pp. 53-78). Springer, Cham.

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, *34*(3), 231-245.

Rokven, J., Boer, G. de, Tolsma, J., & Ruiter, S. (2017). How friends' involvement in crime affects the risk of offending and victimization. *European Journal of Criminology*.

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, *23*(2), 112–137.
Statissta. (2021). Report. Retrieved May, 5, 2021, from https://www.statista.com/
Veresha, R. (2018). Preventive measures against computer related crimes: Approaching an individual. *Informatologia*, *51*(3–4), 189–199.
Wall, D. S. (2012). The devil drives a Lada: The social construction of hackers as cybercriminals. *In Constructing Crime* (pp. 4-18). Palgrave Macmillan, London.
Wall, D. S. (2004). Digital Realism and the Governance of Spam as Cybercrime. *European Journal on Criminal Policy and Research*, *10*(4), 309–335.
Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124.
Wall, D. (2003). *Crime and the Internet*. Routledge.
Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*.

CRIMINOLOGICAL ASPECTS OF THE INTERNET AND ITS ROLE IN CYBER CRIME

Biljana Dimitrić

University PIM, Faculty of Law, Despota Stefana Lazarevića bb, 78 000 Banja Luka, Bosnia and Herzegovina, biljanazdimitric@gmail.com

ABSTRACT

Due to its many characteristics, the Internet deserves special attention in criminology, as well as criminal law and politics. Today, the Internet has become a global, current, interactive module and a civilizational apparatus that enables automated information processing. Due to its various features, the Internet provides unique opportunities for cybercrime, which includes the use of computer networks to achieve this goal. This paper offers an overview of research on how and why the Internet provides unique opportunities for criminal activities, as well as what this means for the management of (cyber) crime or high-tech crime. It outlines some typologies of cybercrime and lists certain risk factors on the Internet that, when combined, create a specific incentive framework for crime. The paper itself briefly addresses the threats and vulnerabilities of law enforcement and other countermeasures, as well as what little is known about cybercriminals, organized cybercrime, and cyber victims. Despite the scarcity of empirical studies on cybercrime, ie cybercrime, the theoretical findings and hypotheses presented in the literature support the conclusion that the Internet is changing crime and that a new kind of adaptability is being created. Research indicates that cybercrime is becoming more organized, more extensive and diverse, with an increasing division of labor and that it is increasingly in synergy with so-called offline organized crime. Moreover, there appears to be a large correlation between offline and online victimization in certain offenses. Now that the use of the Internet has become commonplace in everyday life, criminology, as well as criminal law and politics, should more often include the Internet and cybercrime in their daily practice, while focusing even more on the peculiarities and nuances of the Internet as a special phenomenon.

Keywords: criminology, law, internet, cybercrime.