Dr. sc. iur. Mirza Dinarević
BH Telecom d. d. Sarajevo
Lejla Softić, dipl. iur.
lsoftic085@gmail.com

UDK 004.738.5:343.9

Stručni članak

RAZVOJ, POJAM I OBLICI CYBER KRIMINALA

DEVELOPMENT, CONCEPT AND FORMS OF CYBER CRIME

Sažetak
Cyber kriminal u najširem smislu je svaka kriminalna aktivnost koja uključuje računar, umreženi uređaj ili mrežu. Specifičnost i značaj cyber kriminala je vrlo teško iskazati singularnom definicijom zbog visoke složenosti kriminalnih aktivnosti kao i pravnih posljedica koje uzrokuje. Zbog lakoće pristupa informacijama i zloupotrebe društvenih mreža, cyber kriminal bi mogao postati dominantan vid kriminala. Jedan od motiva na strani razvoja ovog kriminala jeste i ostvarivanje velikog profita. U regulaciji cyber kriminala i njegovih pojavnih oblika mnogo više aktivnosti poduzima se na međunarodnom nego na nacionalnom planu. Kao posljedica masovnog pojavljivanja i razvijanja cyber kriminala nastaju učinkovitija unutarnja i vanjska zaštita podataka kao i pravni okvir za zaštitu podataka.

***Ključne riječi**: cyber kriminal, internet, zakonska regulativa, krivično djelo, peer-to-peer.*

Summary
Cybercrime in the broadest sense is any criminal activity that involves a computer, networked device, or network. The specificity and significance of cybercrime is very difficult to express by one definition, due to the great complexity of criminal activities as well as the legal consequences it causes. Due to the ease of access to information and the misuse of social networks, cybercrime could become the most dominant form of crime. One of the motives on the side of the development of this crime is making a big profit.
Much more action is being taken internationally than nationally to regulate cybercrime and its manifestations. As a consequence of the mass emergence and development of cybercrime, more effective internal and external data protection is emerging, as well as legal data protection.

***Keywords:** cybercrime, Internet, legislation, crime, peer-to-peer.*

1. Uvod

Internet-tehnologija današnjice mnogobrojnim korisnicima olakšava život u raznim segmentima putem društvenih mreža, internet-bankarstva i drugih platformi. Zbog ubrzanog razvoja računarske tehnologije, krivična djela visokotehnološkog kriminala predstavljaju aktuelnu, negativnu društvenu pojavu. Sa sve većim napredovanjem internet-tehnologije uporedo napreduju i neumoljivo se pojavljuju sigurnosne prijetnje sistemima i mrežama. Međunarodni krivičnopravni okvir je zbog pojavljivanja različitih krivičnih djela u cyber prostoru i postepenog uvođenja zakona imao nekoliko faza razvoja. Razvoj međunarodnog krivičnopravnog okvira uključuje sljedeće faze: zaštitu privatnosti, zaštitu nematerijalnih dobara (računarski imovinski kriminalitet), zaštitu intelektualnog vlasništva te zabranu širenja štetnog i ilegalnog sadržaja.

Krivična djela iz oblasti cyber kriminala u Bosni i Hercegovini regulisana su entitetskim zakonodavstvom: Krivičnim zakonom Federacije Bosne i Hercegovine i Krivičnim zakonom Republike Srpske. Prema Ministarstvu sigurnosti Bosne i Hercegovine, djela koja se ubrajaju u cyber kriminal su: ometanje rada sistema i elektronske obrade podataka, prijevare na internetu, neovlašten pristup zaštićenom sistemu i mreži elektronske obrade podataka, krivotvorenje kreditnih i ostalih kartica bezgotovinskog načina plaćanja, posjedovanje i distribucija dječije pornografije, krivična djela u vezi sa zloupotrebama wireless mreža te društvenih mreža, krivična djela povrede autorskih prava. U Bosni i Hercegovini sve češća je i pojava ekonomske špijunaže, širenja malwarea, neovlaštenog upada u zaštićene sisteme, krađe bankovnih kartica, a najčešća pojava su različiti oblici internet-prijevara.[1]

2. Pojam i podjela cyber kriminala

Do inicijative za određivanje pojma računarskog kriminala došao je U.S. Senate Government Operations Committee 1977. godine.[2] Prva međunarodna organizacija koja se bavila problemom računarskog kriminala i legislative je Interpol. 1981. godine održana je Interpolova konferencija te su identificirani potencijalni problemi. Vijeće Evrope je 1985. uspostavilo još jedan komitet sastavljen od eksperata, kako bi se razgovaralo o računarskom kriminalu, nakon čega su 1989. godine donesene i konkretne preporuke. UN je 1990.

[1] *Edukator: naučno-stručni i informativni časopis*, Travnik, Univerzitet/Sveučilište „Vitez“, 2016, str. 1.
[2] Američki odbor za upravljanje Senatom.

godine donio i rezoluciju o računarskom kriminalu. Rezolucija je postala vrlo bitan element kod izrade strategija ili Zakona o računarskom kriminalu u EU i skoro sve evropske zemlje su potpisale ovu rezoluciju. Bosna i Hercegovina ovu rezoluciju je prihvatila i ratificirala 2006. godine.

Zbog različitih pristupa nastaju poteškoće u definisanju pojmova „računarski kriminal" i „cyber kriminal", s obzirom na to da se odnose na opisivanje niza krivičnih djela: tradicionalnih računarskih krivičnih djela i mrežnih krivičnih djela. Budući da se ta krivična djela razlikuju na mnogo načina, ne postoji jedinstveni kriterij koji bi uključivao sve radnje spomenute u različitim međunarodnim pravnim okvirima. Umjesto definicije moguće je služiti se tipološkim pristupom, kao što je definisano u Konvenciji Vijeća Evrope.

U Evropskoj konvenciji o računarskom kriminalu navode se četiri grupe djela: **djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema (nezakoniti pristup, presretanje, uplitanje u podatke, korištenje uređaja, programa), djela vezana za kompjutere (falsifikovanje i krađe), djela vezana za sadržaje (najčešće se javlja u obliku dječije pornografije, a obuhvataju posjedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim ovih materijala) i djela vezana za kršenje autorskih prava.**[3]

3. Nastanak i razvoj cyber kriminala

Pojmovi „haker" i „hakovanje" postali su općepoznati i predstavljaju jedan od najčešće analiziranih oblika cyber kriminala. Zajednička definicija nastala raspravom stručnjaka o hakovanju je: „Hakovanje je neovlašteni pristup i naknadna upotreba tuđeg računarskog sistema." Zlonamjerna povezanost s hakerima (izvorni prijevod s njemačkog jezika – neko ko pravi namještaj sa sjekirom) postala je očita 1970-ih u SAD-u, kada su rani kompjuterizovani telefonski sistemi postali meta. Pojam „haker" tada se smatrao pozitivnim te je opisivao osobu nadprosječnih vještina u razvijanju kreativnih, elegantnih te djelotvornih rješenja računarskih problema. Dodatno, „hack" je sam po sebi označavao inovativno korištenje tehnologije koje je dovelo do pozitivnih rezultata i prednosti.

[3] Dostupno na: https://ire.ba/sta-znamo-o-cyber-kriminalu/.

Prema programerskom leksikonu *The Jargon File*, haker je osoba koja:

– uživa istraživati detalje računarskih programa i traži način da poveća učinkovitost sistema, za razliku od ostalih korisnika koji uče i koriste samo osnove programa,
– programira s posebnim entuzijazmom ili osoba koja više uživa u programiranju nego u raspravljanju o istom,
– cijeni vrijednosti pravog hacka,
– brzo programira,
– je stručnjak za neki korisnički program.

Tehnološki upućeni pojedinci, zvani „freakers“, otkrili su ispravne kodove i tonove koji bi rezultirali besplatnom uslugom na velikim daljinama. Oni su se lažno predstavljali, iskopali „otpad“ kompanije Bell Telephone da pronađu tajne informacije i izveli bezbrojne eksperimente na ranom telefonskom hardveru, sa ciljem da nauče iskoristiti sistem i ukrasti telefonsko vrijeme na duže staze. Vishing (glas ili VoIP phishing) je elektronska prijevara u kojoj se pojedinci uvlače u otkrivanje kritičnih finansijskih ili ličnih podataka neovlaštenim subjektima. Vishing djeluje poput krađe identiteta i provodi se pomoću govorne tehnologije. Napad se može izvesti glasovnom e-poštom[4], VoIP-om (glas preko IP-a) ili fiksnim ili mobilnim telefonom. Vishing je uvjerljiv trik koji koristi zastrašujuće taktike za pritisak sa ciljem saznanja ličnih podataka. Kradljivci identiteta koriste lične podatke kako bi otvorili račune, pokrenuli dug i zloupotrijebili kredit žrtve. Prevaranti se mogu pretvarati da potječu iz legitimnih finansijskih institucija, kompanija ili vladinih agencija. Oni traže povjerljive podatke kao što su brojevi finansijskih računa i kreditnih kartica, brojevi socijalnog osiguranja, lozinke i lični identifikacijski brojevi.

Ova inovativna vrsta kriminala predstavljala je težak izazov za provođenje zakona, dijelom i zbog nedostatka zakona, kao i zbog manjka istražitelja koji su vješti u tehnologiji koja se hakuje. Bilo je jasno da su računarski sistemi otvoreni za kriminalne aktivnosti, a sa porastom komunikacijskih sredstava proširene su i mogućnosti za cyber kriminal.
Sistemski administrator Clifford Stoll, u laboratoriji Lawrence Berkeley, uočio je 1986. određene nepravilnosti u računovodstvenim podacima. Izumivši prve digitalne forenzičke tehnike, utvrdio je da neovlašteni korisnik upada u njegovu računarsku mrežu. Stoll je koristio tzv. „taktiku saća“, koja

[4] Elektronska pošta, e-pošta ili e-mail (engl. electronic mail) prijenos je tekstualnih poruka (moguće je prilagati i dokumente koji nisu tekstualni) putem komunikacijskih mreža, najčešće interneta.

hakera vraća u mrežu dok se ne prikupi dovoljno podataka za praćenje neovlaštenog upada u njegov izvor. Stollovo otkriće je rezultiralo hapšenjem Markusa Hessa i nekolicine drugih smještenih u zapadnoj Njemačkoj, koji su krali i prodavali vojne podatke, lozinke i druge podatke sovjetskom KGB-u.

Nakon upada u laboratoriju u Berkeleyu ubrzo je uslijedilo otkriće virusa crva Morris, koji je stvorio Robert Morris, student Univerziteta Cornell. Ovaj virus je oštetio više od 6.000 računara i prouzrokovao štetu od cca 98 miliona dolara. Incidenti su se nastavili nizati neprekidnim i nesmetanim tokom. Američki Kongres je odreagovao donošenjem svoje prve legislative u vezi sa hakovanjem Federalnog zakona o prijevarama i zloupotrebama računara 1986. Tim činom su krivična djela iz grupe cyber kriminala sankcionisana kaznama zatvora i novčanim kaznama.

Smrt kritično bolesne pacijentice u Njemačkoj nakon cyber napada mogla bi biti prvi poznati slučaj gubitka života usljed hakovanja. Pacijentica je trebala biti liječena u Univerzitetskoj bolnici u Düsseldorfu 11. septembra, ali napad ransomwarea dan ranije izmiješao je podatke i onemogućio rad računarskih sistema u bolnici. Kao rezultat hakovanja ljekari nisu mogli primiti pacijenticu i morali su je prebaciti u drugu bolnicu udaljenu 30 km. Putovanje je spriječilo ženu da dobije spasonosni tretman koji joj je bio toliko potreban i preminula je u bolnici u Wuppertalu. Tužitelji u Kölnu službeno su pokrenuli slučaj ubistva iz nehata ustvrdivši da bi hakeri mogli biti krivi. Detektivi trenutno sarađuju sa stručnjacima za cyber sigurnost, kako bi utvrdili postoji li veza između hakovanja i pacijentove smrti. Ciaran Martin, bivši izvršni direktor britanskog Nacionalnog centra za cyber sigurnost, rekao je da će, ukoliko se utvrdi da su hakeri odgovorni, to označiti kao prvu smrt izravno uzrokovanu cyber napadom. Arne Schönbohm, predsjednik njemačkog nacionalnog tijela za cyber sigurnost, rekao je da su dužnosnici došli na lice mjesta kako bi pomogli IT-osoblju bolnice u obnovi sistema. Upozorio je druge organizacije da se bolje zaštite, jer su hakeri iskoristili poznatu ranjivost u dijelu softvera VPN (virtuelna privatna mreža), koji je razvio Citrix, prenosi BBC News. U izjavi je Schönbohm komentarisao: „Već smo u januaru upozorili na ranjivosti sistema i ukazali na moguće posljedice. Napadači mogu dobiti pristup internim mrežama i sistemima, te ih još mogu paralizovati mjesecima kasnije. Mogu samo naglasiti da takva upozorenja ne treba zanemariti, već odmah treba poduzeti odgovarajuće mjere. Ovaj incident još jednom pokazuje koliko ovaj rizik mora biti ozbiljno shvaćen.“ Martin je rekao da nije iznenađujuće što je uzrok problema u računarskom sistemu bio kriminalni ransomware napad, a ne teroristički napad. Nastavio je: „Iako je svrha ransomware napada zaraditi novac, ipak takav napad zaustavlja rad sistema. Dakle, ako napadnete bolnicu, onda će se takve stvari vjerovatno dogoditi. Ranije ove godine bilo je

nekoliko neuspješnih pokušaja širom Evrope, ali sada se nažalost izgleda dogodilo najgore. Lokalni izvještaji koje je citirao BBC sugerišu da hakeri nisu namjeravali napasti bolnicu, već su pokušavali napasti drugi univerzitet. U digitalnoj poruci poslanoj tokom napada hakeri zahtijevaju plaćanje od Univerziteta Heinrich Heine, povezanog, ali različitog mjesta od bolnice. Nakon što su uvidjeli svoju pogrešku, navodno su dali bolnici ključ za dešifriranje bez zahtjeva za plaćanjem, a zatim su nestali. Internet nudi globalno tržište za potrošače i kompanije na kojem vršioci internet-prijevara prepoznaju potencijale žrtve cyber prostora.[5]

Iste prijevare koje su ranije vođene putem pošte i telefona sada se mogu naći na World Wide Webu[6] i u e-pošti, a pojavljuju se i nove cyber prijevare. Ponekad je teško utvrditi razliku između uglednih internetskih prodavača i kriminalaca koji koriste internet kako bi opljačkali ljude, zbog čega je potrebno naučiti prepoznati znakove opasnosti prijevara.

4. Peer-to-peer mreže

Peer-to-peer mreže pružale su neprocjenjivu uslugu koja korisnicima omogućava razmjenu informacija i podataka širom svijeta. Te su mreže postale popularne za dijeljenje medija, a kulminirale su zloglasnim Napsterovim skandalom. Napster je set od tri mrežne usluge fokusirane na muziku. Osnovan je 1999. godine kao pionirski peer-to-peer (P2P) internetski softver za razmjenu datoteka koji naglašava dijeljenje digitalnih audiodatoteka, obično audiopjesama, kodiranih u MP3-formatu. Kako je softver postao popularan, kompanija je naišla na pravne poteškoće zbog kršenja autorskih prava. Prestao je s radom i na kraju ga je preuzeo Roxio. Napster je postao internetska muzička trgovina. Američko udruženje snimateljske industrije (RIAA) burno je reagovalo na Napsterovu olakšicu prenošenja materijala zaštićenih autorskim pravima kada je 6. decembra 1999. pokrenulo tužbu protiv popularne usluge. Napster je imao poslužitelja, ali on je imao ulogu spajanja dvaju klijenata koji bi onda međusobno razmjenjivali

[5] Engl. cyberspace: pojam je književnog porijekla, prvi put spomenut u romanu *Neuromancer* Williama Gibsona. Naziva se još kibernetičkim prostorom, a označava virtuelnu stvarnost. Cyber prostor je prostor uspostavljen uz pomoć i posredovanje kompjutersko-digitalne tehnologije. Pojam kibernetičkog prostora ili cyberspacea danas se koristi za sve što je na internetu.

[6] Skraćeno WWW, W3, ili samo Web; naziv dolazi iz engleskog jezika – razgranata mreža, a može se prevesti kao „svjetska mreža“; WWW je jedna od najkorištenijih usluga interneta koja omogućava pregled hipertekstualnih dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje.

podatke, tako da se može reći da je Napster prvi pravi peer-to-peer sistem na internetu. Ipak, pod pritiskom tužbi Napster je nesretno završio i bankrotirao. Nakon Napstera dolazi Gnutella koja je funkcionisala bez poslužitelja, a za spajanje na nju je bila potrebna adresa bilo kojeg računara unutar mreže. Međutim, pravu revoluciju u peer-to-peer mrežama je donio BitTorrent protokol za razmjenu podataka, koji je razvio Bram Cohen. Veliko rasterećenje i brzina mreže postižu se u njemu tako da svi povezani klijenti koji imaju određenu datoteku šalju je u dijelovima onima koji traže tu datoteku. Time je poslužitelj znatno rasterećen te se brzina razmjene povećava ovisno o broju korisnika. Nakon BitTorrenta razvijeni su i brojni slični protokoli, preko kojih se danas odvija veći promet od onoga koji koriste servisi klijent – poslužitelj.[7]

Postoji određena svijest o problemu sa autorskim pravima koji nastaje upotrebom peer-to-peer dijeljenja medija. Međutim, postoje i drugi problemi s cyber kriminalom kojima se korisnici mogu izložiti pri korištenju peer-to-peer mreža. Peer-to-peer mreže mogu se koristiti na više ispravnih načina, ali korisnici se moraju zaštititi od cyber kriminala koji prevladava u istim mrežama.

Najčešće se peer-to-peer mrežama pristupa putem besplatnog softvera koji omogućava korisniku da pronađe i preuzme datoteke na računaru drugog korisnika. Tradicionalna računarska mreža koristi model klijenta i poslužitelja, u kojem klijentski računari pohranjuju i pristupaju podacima na namjenskom poslužitelju. Peer-to-peer mreže odmiču se od namjenskog poslužitelja. Dakle, svaki računar je klijent i server. To omogućava svakom korisniku da pristupi i dijeli informacije direktno umjesto kroz središnji koncentrator. Te mreže također pružaju korisnicima veću kontrolu. Korisnici mogu odlučiti na koje će se računare povezati, koje datoteke dijeliti i koliko sistemskih resursa posvetiti mreži. Korisnici imaju brojne kontrole nad peer-to-peer mrežom. Međutim, prosječni korisnik može se izložiti opasnosti i olako postati žrtva cyber kriminala ukoliko nije dovoljno upućen u kontrolisanje mrežnih postavki.

Najpoznatija problematika u upotrebi mreža peer-to-peer je kršenje autorskih prava. Dijeljenje muzike, filmova i softvera zaštićenog autorskim pravima krši zakone o autorskim pravima. Dijeljenje ovih materijala zaštićenih autorskim pravima može izložiti korisnika krivičnim sankcijama. Ipak, mnogi peer-to-peer korisnici ne krše zakone o autorskim pravima. Ali, čak i uz zakonitu upotrebu, korisnici mogu postati žrtve cyber kriminala. Hakeri često koriste

[7] E. Markovinović, Peer to peer mreže, završni rad, Sveučilište J. J. Strossmayera, Osijek, 2015, str. 5.

otvorenost peer-to-peer mreža za pristup drugim računarima. Mnogi hakeri posebno stvaraju viruse koji se šire putem mreža. Virus je program ili kôd koji se prikači na program ili datoteku, tako da može da se prenosi sa računara na računar šireći pritom zarazu. Virusi mogu oštetiti softver, hardver i datoteke. Virus je kôd napisan sa jasnom namjenom da sâm sebe umnožava. Virus pokušava da se širi od računara do računara tako što se kači na neki program. Među računarskim virusima postoje oni koji su samo mala smetnja pri radu do onih koji su potpuno destruktivni.[8] Virus se obično sastoji od tri dijela:

> – prvi dio je dio koji omogućava razmnožavanje virusa – obvezan dio virusa,
>
> – drugi dio je nosiva komponenta (payload) koja može biti bezopasna ili opasna – nije obavezna,
> – treći dio je funkcija za okidanje ili takozvana trigger funkcija – određuje vrijeme (a ponekad i događaj) kada će se aktivirati nosiva komponenta virusa – nije obavezna.[9]

Bez ispravnog konfigurisanja peer-to-peer softvera, hakeri će moći pristupiti računaru, omogućavajući pregled i preuzimanje informacija direktno sa hard diska. Računarski kriminal može se podijeliti i na: **politički** (cyber špijunaža, haking, cyber sabotaža, cyber terorizam, cyber ratovanje), **ekonomski** (cyber prijevare, haking, krađa internet-usluga i vremena, piratstvo softvera, mikročipova i baza podataka, cyber industrijska špijunaža, lažne internet-aukcije), **proizvodnja i distribucija nedozvoljenih i štetnih sadržaja** (dječija pornografija, pedofilija, vjerske sekte, širenje rasističkih i nacionalističkih ideja i stavova, zloupotreba žena i djece, trgovina ljudskim organima, oružjem i drogom) i **povrede cyber privatnosti** (nadgledanje elektronske pošte, spam, prisluškivanje i snimanje).[10]

Pod cyber kriminalom u širem smislu podrazumijeva se svaka kriminalna aktivnost koja uključuje računar, umreženi uređaj ili mrežu. Dok se većina cyber kriminala provodi sa ciljem stvaranja zarade, određeni cyber zločini provode se nad računarima ili uređajima direktno kako bi ih oštetili ili onemogućili, dok drugi koriste računare ili mreže za širenje zlonamjernog softvera, ilegalnih podataka, slika ili drugog materijala. Pojedini cyber zločini

[8] Dostupno na: https://www.sergije-stanic.me/images/Racunarski_virusi2014-2015.pdf.
[9] Dostupno na: https://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_virus.
[10] Dostupno na: https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala.

obuhvataju i jedno i drugo, tj. ciljaju računare kako bi ih zarazili virusom, koji se zatim širi na druge uređaje, a ponekad i na čitave mreže.[11]
Šire definicije pokušavaju precizirati ciljeve i namjere i tačnije definisati cyber kriminal, npr.:

> – cyber kriminal su krivična djela koja se odnose na kibernetičke sisteme (kibernetički sistem je skup elemenata međusobno povezanih vezama koji djeluju jedan na drugi. Kibernetički sistem može biti biološki, društveni, tehnički i bavi se problemom upravljanja, regulisanja i obrade informacija u tehničkim sistemima);[12]
> – cyber kriminal su računarski posredovane aktivnosti koje su ili nezakonite ili se smatraju nedopuštenim od određenih interesnih skupina i koje se mogu provoditi putem globalnih računarskih mreža.[13]

Ovakvim definicijama isključuju se klasična krivična djela u kojima se pojavljuje računar kao sredstvo počinjenja krivičnog djela ili kao dio dokaza, ali isto tako nose rizik da isključe određena krivična djela koja se smatraju cyber kriminalom u određenim međunarodnim sporazumima, poput npr. Konvencije Vijeća Evrope o kibernetičkom kriminalu. Kada bi osoba pomoću zlonamjernih računarskih programa na prijenosnom uređaju USB obrisala podatke na računarskom sistemu, to djelo ne bi bilo okvalificirano kao cyber kriminal prema tim definicijama, jer nije počinjeno korištenjem računarskih mreža.
Hart je u svom djelu „Koncept zakona“ napisao da su „ljudska bića ranjiva pa je za njihovu zaštitu potrebna vladavina zakona.“ Primjenjujući isto na cyber prostor, možemo reći da su računari ranjivi pa je potrebna vladavina zakona da bi ih zaštitila od cyber kriminala. Razlozi ranjivosti računara su:

1. kapacitet za pohranu podataka u relativno malom prostoru:
Računari imaju jedinstvenu karakteristiku za pohranu podataka u vrlo malom prostoru, što omogućava mnogo lakši pristup ili uklanjanje informacija putem fizičkih ili virtuelnih medija.

2. olakšan pristup:
Problemi u zaštiti računarskih sistema od neovlaštenih pristupa su u mogućnostima neovlaštenog pristupa, ne zbog ljudske pogreške, nego zbog složene tehnologije. Potajno ugrađenom logičkom bombom, ključnim

[11] M. Gerecke, Understanding cybercrime, Phenomena, challenges and legal response, Telecommunication Development Sector, 2012, str. 11–14.
[12] P. Cornish, R. Hughes and D. Livingstone, Cyberspace and the National Security of the United Kingdom, 2009, Chatham House, str. 1–7.
[13] E. Tamarkin; Cybercrime, Institute for Security studies, USA, 2014, str. 2.

kodiranim zapisima koji mogu ukrasti pristupne kodove, naprednim diktafonima mrežnice i sl. koji mogu zavaravati biometrijske sisteme i zaobilaziti vatrozide (engl. firewall; mrežni uređaj čija je namjena filtriranje mrežnog prometa tako da se stvori sigurnosna zona. Program koji želi pristupiti internetu treba imati dopuštenje od vatrozida. Obično se kombiniraju usmjernici i sigurnosne stijene, kao jedan uređaj, ili se kaskadiraju, npr. unutarnja, osigurana mreža – sigurnosna stijena – usmjernik – vanjski svijet mogu se upotrijebiti da bi se premostili mnogi sigurnosni sistemi).

3. nepažnja:
Nepažnja je usko povezana s ljudskim ponašanjem. Stoga je vrlo vjerovatno da prilikom zaštite računarskog sistema može doći do nepažnje, što zauzvrat hakeru omogućuje pristup i nadzor nad računarskim sistemom.

4. gubitak dokaza:
Gubitak dokaza vrlo je čest i očit problem, jer se svi podaci rutinski uništavaju. Daljnje prikupljanje podataka izvan teritorijalnog opsega također paralizira ovaj sistem istrage kriminala.

5. Phishing napadi

Lažno predstavljanje jedna je od najučinkovitijih i najpoznatijih cyber prijevara. Lažno predstavljanje postaje sve opasnije razvijanjem u sofisticirane napade koji mogu manipulisati korisnicima putem prevarantskih veb-stranica, ciljanih poruka e-pošte i lažnih telefonskih poziva.[14]

Incidenti u vezi sa krađom identiteta, poput slučaja „John Podesta“, u konačnici pokazuju da, bez obzira na tehničko znanje i pozadinu korisnika, svako, bez razlike, može postati žrtva ovih napada, a posljedice mogu biti ogromne. Lažno predstavljanje uspješno je jer napadači manipulišu svojim ciljevima, na način da privuku korisnike obećavajući im posebne koristi ili prisiljavajući korisnike koristeći se prijetnjama. Takve manipulativne tehnike često dovode do impulsivnog ili brzog donošenja odluka krajnjih korisnika. Jedna od najčešćih motivacija za krađu identiteta je obećanje finansijske koristi žrtvi. Pojam krađe identiteta nastao je 1996. godine, kada su hakeri krali podatke s interneta sa američkih računa. Ovi hakeri su koristili e-poštu kao „kuke“, kako bi uhvatili svoju „ribu“ iz „mora“ korisnika interneta.

[14] L. James, Phishing exposed, Secure Science Corporation, USA, 2005, str.10–13.

Pojam „phishing“ dolazi od engleske riječi „fishing“ kojom se metaforički opisuje postupak kojim neovlašteni korisnici mame korisnike interneta, kako bi dobrovoljno otkrili svoje povjerljive podatke. Pretpostavka je da prefiks *ph-* dolazi od termina „phreaking“, tehnike kojom su neovlašteni korisnici kompromitirali telefonske sisteme. Phishing napadi podrazumijevaju aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektronske pošte i lažiranih veb-stranica finansijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih ličnih podataka. Pritom se prvenstveno misli na podatke kao što brojevi kreditnih kartica, korisnička imena, PIN-kodovi i sl., iako postoje i druge alternative.[15] Danas postoji nekoliko vrsta phishing napada, poput prijevarne krađe identiteta, krađe identiteta na zlonamjernom softveru, Keyloggera i Screenloggera, hakovanje, web trojanski podaci, krađe identiteta u tražilicama, krađe identiteta u obliku injekcije, krađe identiteta na bazi DNS-a...

Postoje tri glavne faze u phishing ciklusu. U prvoj fazi phisher (napadač) istražuje i bira organizacije, zatim stvara phishing veb-stranicu i šalje brojne neželjene e-poruke između različitih korisnika internet-zajednice. Druga faza započinje čitanjem ovih poruka e-pošte. Kad god korisnik „ugrize“ na *phishu*, tj. klikne na vezu, započinje treća faza i korisnik je preusmjeren na phishing mjesto. Često se pružaju sigurnosni alati i upozorenja kao rješenje za ublažavanje takvih napada.

Na strani korisnika postoje različita rješenja: pojedine aplikacije zasnovane na „crnoj listi” blokiraju veb-lokaciju ako domen potpada pod crnu listu. Za razliku od rješenja na crnoj listi, za e-poruke koje blokiraju e-poštu prije nego što dođu do poslužitelja pošte SMTP[16], blokira veb-mjesto kada pretraživač zahtijeva klijenta za URL naveden na popisu. Određena rješenja poput heurističkih značajki i vizuelne sličnosti blokiraju veb-stranicu samo kada preglednik zatraži bilo koju veb-stranicu za krađu identiteta.

Prilikom izvršenja zakonskih propisa koji se odnose na krađu identiteta nailazi se na određene poteškoće. Prva poteškoća jeste nedostatak resursa. Istražitelji u agencijama za provođenje zakona najčešće zaostaju za cyber kriminalcima u smislu nedovoljnog razumijevanja tehnologije i opreme kojom oni raspolažu. Pored toga, krađa identiteta je najčešće podijeljena na više osoba, najčešće su u pitanju različite države, zbog čega postoji više aspekata tog napada, naprimjer pružajući upute za sam napad, pomažući postavljanje

[15] Phishing napadi, Akademska i istraživačka mreža HR – CARNet, str. 4.
[16] SMTP, od engl. Simple Mail Transfer Protocol, uobičajeni je način (de facto standard) za prijenos elektronske pošte na internetu.

stranica za prijevare, slanje i pranje e-maila. Ipak, najveći problem predstavlja nadležnost. Zbog višenacionalne i višedržavne prirode samog cyber napada, državni i federalni zakoni mogu imati ograničene nadležnosti.

6. Zakonska regulativa cyber kriminala

Iako održiva politika cyber sigurnosti uključuje širok spektar tema za razmatranje, zakonske mjere igraju ključnu ulogu u prevenciji i borbi protiv cyber kriminala. One su potrebne u svim oblastima, uključujući inkriminaciju, procesna ovlaštenja, nadležnosti, međunarodnu saradnju i odgovornosti pružatelja internetskih usluga.
Konkretno, na nivou države zakoni o cyber kriminalu najčešće se tiču inkriminacije – utvrđivanja specifičnih krivičnih djela za osnovne radnje cyber kriminala. Države, međutim, sve više prepoznaju potrebu za zakonodavstvom i u ostalim područjima.
U mnogim državama zakoni o tehničkim dostignućima datiraju još iz 19. vijeka. Ti su zakoni bili, i u velikoj su mjeri i dalje, usredotočeni na fizičke objekte – oko kojih se vrtio svakodnevni život industrijskog društva. Iz tog razloga mnogi tradicionalni opći zakoni ne uzimaju u obzir posebnosti informacija i informacione tehnologije koji su povezani sa cyber kriminalom. Djela ove prirode su uglavnom karakterizirana novim nematerijalnim objektima, kao što su podaci ili informacije. Iako se krivični zakon često smatra najrelevantnijim kada je u pitanju cyber kriminal, pravni odgovori na širu zabrinutost zbog cyber sigurnosti zahtijevaju i angažman drugih grana prava, kao što su građansko pravo i upravno pravo. Najviše zakona o cyber kriminalu obično se nalazi u oblastima materijalnog i procesnog krivičnog prava.
Pitanje inkriminacije nepoželjnog ponašanja na internetu ima dvojaki učinak:

1. stvaranje pravne osnove za retributivno suzbijanje ponašanja i
2. stvaranje klime društvene neprihvatljivosti cyber kriminala koja bi trebala da stigmatizira takve oblike ponašanje.

Inkriminacija (određivanje krivičnog djela)

Na nacionalnom nivou najčešće postojeći i novi (ili planirani) zakoni o cyber kriminalu tiču se inkriminacije, što ukazuje da je fokus stavljen na definisanje posebnih krivičnih djela. Globalno, mnoga zakonodavstva imaju tendenciju da svoj krivični i procesni zakonski okvir smatraju sasvim dovoljnim, iako takvi stavovi doprinose prikrivanju velikih regionalnih razlika. Također, iako

postoji konsenzus na visokom nivou o potrebi prepoznavanja štetnih radnji i njihovom određivanju kao krivičnih djela, sama zakonska rješenja na nivou države otkrivaju različite pristupe. Tako npr. krivična djela koja uključuju ilegalni pristup računarskim sistemima i podacima u pojedinim zakonodavstvima mogu se posmatrati različito u odnosu na predmet krivičnog djela (podaci, sistemi ili informacija), pri čemu je u pojedinim zakonodavstvima dovoljno izvršiti radnju pukog pristupa, dok druga zakonodavstva mogu tražiti dodatne elemente namjere prouzrokovanja gubitka ili štete. Pristupi se razlikuju i kada su u pitanju djela ometanja računarskih sistema i podataka. Većina država zahtijeva da ometanje bude namjerno, dok postoje i primjeri zakonskih rješenja koji inkriminišu i nepromišljeno ometanje.

Također, alati za izvršenje djela cyber kriminala nisu inkriminisani u svim državama. Za one koji to čine nastaju daljnje razlike u vezi s tim uključuje li krivično djelo posjedovanje, širenje ili upotrebu softvera (kao što je zlonamjerni softver) i/ili računarske pristupne šifre (poput lozinki žrtve). Iz perspektive međunarodne krivičnopravne saradnje takve razlike mogu imati velikog utjecaja na procesuiranje počinitelja takvih krivičnih djela. Prekogranična priroda cyber kriminala i počinjenje djela u virtuelnom okruženju glavne su poteškoće s kojima se policija suočava. Cyberspace čini fizički prostor irelevantnim. Nastali su novi izazovi u istrazi od inovacija počinitelja, poteškoća u pristupu elektronskim dokazima kao i zbog internih kapaciteta i logističkih ograničenja policijskih službi. Počinitelji često koriste tehnologije anonimizacije, a nove tehnike jako brzo se šire internetskim bespućima, što značajno otežava istragu.[17] Identifikacija počinioca, istraga i prikupljanje dokaza o krivičnom djelu mogu biti teški iz različitih razloga. Pored izazova anonimizacije i prikrivanja, država koja je domaćin cyber kriminalca i njegove aktivnosti možda njegovu radnju ne definiše kao krivično djelo, te stoga možda neće biti u mogućnosti da ga krivično goni ili sarađuje u njegovom izručenju za krivično gonjenje drugdje; država domaćin možda nema važeće ugovore sa državom u kojoj je djelo počinjeno, koji bi je obavezivali da pomogne u prikupljanju dokaza koji se mogu koristiti protiv počinilaca.

[17] A. Appazov, Legal Aspects of Cybersecurity, Faculty of Law, University of Copenhagen, Copenhagen, 2014, str. 34–36

Harmonizacija

Mnoge zemlje imaju zakonska rješenja koja se bave cyber sigurnošću i cyber kriminalom, ali ti se pravni okviri u velikoj mjeri razlikuju u pogledu načina na koji se rješavaju ova pitanja. U današnjem globaliziranom svijetu zakonska regulativa sastoji se od mnoštva državnih, regionalnih i međunarodnih pravnih sistema. Interakcije između ovakvih sistema javljaju se na više nivoa. Kao rezultat, odredbe su ponekad u suprotnosti, što dovodi do kolizije zakona ili se rješenja ne poklapaju dovoljno, ostavljajući pravne praznine. Usklađivanje zakonodavnih rješenja može se poduzeti na nekoliko načina, uključujući i obavezujuće i neobvezujuće međunarodne ili regionalne inicijative. Osnova usklađivanja može biti jedinstveni pristup pojedinih država ili, češće, zajednički pravni elementi identificirani u zakonu niza država ili izraženi u okviru multilateralnog instrumenta, poput ugovora ili neobavezujućeg međunarodnog standarda. Jedan od glavnih argumenata u prilog ujednačavanju zakona među različitim jurisdikcijama je onemogućavanje stvaranja sigurnih utočišta za počinitelje. Dakle, ako su štetna djela u vezi sa korištenjem interneta definisana kao krivična djela, naprimjer, u državi A, ali ne i u državi B, počinitelji u državi B mogu slobodno putem interneta činiti štetu državi. U takvim slučajevima država A ne može se efikasno zaštititi od efekata takvih transnacionalnih aktivnosti. Čak i tamo gdje krivični zakon dopušta utvrđivanje nadležnosti nad počiniocem u državi B, i dalje je potrebno tražiti saglasnost ili pomoć države B – bilo u vezi sa prikupljanjem dokaza ili sa izručenjem identificiranog počinioca. Da bi zaštitila osobe u svojoj jurisdikciji, država B vjerovatno neće pomoći u onim slučajevima koji nisu inkriminisani u njenom zakonodavstvu. Harmonizacija zakonodavstva također može omogućiti globalno prikupljanje dokaza, a usklađivanje procesnog prava je drugi neophodan zahtjev za djelotvornu međunarodnu pravnu saradnju.[18]

7. EU strategije za poboljšanje cyber sigurnosti

Pet strateških prioriteta cyber sigurnosti EU su:

1. postizanje „cyber otpornosti“ uspostavljanjem minimalnih zahtjeva za funkcionisanje, saradnju i koordinaciju nacionalnih nadležnih tijela za mrežne informacijske sisteme,
2. smanjenje internetskog kriminala:
   a) osiguravanjem brze transpozicije EU direktiva povezanih sa cyber kriminalom,

[18] A. Appazov, 40.

b) poticanjem ratifikacije Budimpeštanske konvencije Vijeća Evrope o kibernetičkom kriminalu (Vijeće Evrope 2001) i
c) finansiranjem programa za raspoređivanje operativnih alata,

3. razvijanje politike i sposobnosti za odbrane (Zajednička sigurnosna i odbrambena politika – CSDP):
   a) procjenom operativnih zahtjeva EU za cyber odbranu,
   b) razvojem okvira EU politike cyberdefence,
   c) promicanjem dijaloga i koordinacije između civilnih i vojnih aktera u EU i
   d) omogućavanje dijaloga s međunarodnim partnerima,
4. razvoj industrijskih i tehnoloških resursa za cyber sigurnost:
   a) uspostavljanjem javno-privatne platforme za mrežna i informaciona rješenja (NIS) rješenja,
   b) pružanjem tehničkih smjernica i preporuka za usvajanje NIS-ovih standarda i dobre prakse i
   c) potičući razvoj sigurnosnih standarda za tehnologiju „s jačim, ugrađenim i user-friendly sigurnosnim karakteristikama“,[19]
5. uspostavljanje koherentne međunarodne politike cyber prostora za EU i promicanje osnovnih vrijednosti EU uključivanjem pitanja cyber prostora u vanjske odnose EU i Zajedničku vanjsku i sigurnosnu politiku (CFSP), te podržavanjem izgradnje kapaciteta na cyber sigurnosti i elastičnim informacijskim infrastrukturama u trećim zemljama.

Preciznije, EU bi trebala osigurati da su njene konsultacije s međunarodnim partnerima o cyber pitanjima osmišljene kao dopuna postojećem bilateralnom dijalogu između država članica i trećih zemalja. Ove će se konsultacije voditi osnovnim vrijednostima EU: ljudskim dostojanstvom, slobodom, demokratijom, jednakošću, vladavinom zakona i poštovanjem temeljnih prava. Slijedeći ciljeve ovog prioriteta, EU želi postići visok nivo zaštite podataka, uključujući zaštitu ličnih podataka prenesenih u treće zemlje. Identificirajući ovih pet različitih prioritetnih područja, strategija iz 2013. imala je za cilj „učiniti internetsko okruženje EU najsigurnijim na svijetu“ (Evropska komisija i visoki predstavnik 2013) – na neki način poništavajući kliše da nijedno tehničko okruženje nije stopostotno sigurno. Teško je izmjeriti trenutni kapacitet cyber sigurnosti na nivou EU i da li to djelotvorno rezultira najsigurnijim mogućim internetskim okruženjem. Dva napada ransomwarea, poznata pod imenima WannaCry i Petya (malware), koja su se desila 2017. godine, ukazala su na to da se još uvijek mogu napraviti mnoga

[19] L. Kovacs, Cyber security policy and strategy in the European Union and Nato, National University of Public Service, Budapest, Hungary, 2018, 17–18.

poboljšanja, posebno u pogledu odgovora i saradnje između različitih aktera koji se bave cyber sigurnošću na EU i nacionalnom nivou. Dva spomenuta napada zanimljiva su za razmatranje i iz druge perspektive. Oni predstavljaju posebno dobru demonstraciju niza karakteristika cyber sigurnosti kao područja politike. Prvo, ovo područje politike prepoznaje da su cyber napadi nova stvarnost i da takvi napadi ne samo da mogu imati kaskadne efekte koje je teško predvidjeti već i da mogu osakatiti mnogo više organizacija u Evropi nego što se očekivalo. Istodobno, prepoznavanje ozbiljnosti cyber napada raste nakon cyber incidenata koji nanose štetu preduzećima sa sjedištem u EU. Drugo, suočavanje sa cyber napadima zahtijeva blisku saradnju između dobro uspostavljenih mreža sastavljenih od javnih i privatnih entiteta. Treće, neučinkovite politike za regulaciju područja cyber sigurnosti mogu ometati nesmetano funkcionisanje jedinstvenog digitalnog tržišta, što zauzvrat može imati štetne monetarne implikacije za pojedince, preduzeća i javni sektor. Druga strategija kibernetičke sigurnosti EU iz 2017. naglasila je potrebu za mjerama koje će omogućiti: 1) izgradnju veće otpornosti EU na cyber napade, 2) olakšavanje otkrivanja cyber napada i 3) jačanje međunarodne saradnje na cyber sigurnosti (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku 2017). Zajednička strategija iz 2017. dobro ilustrira evoluciju razumijevanja područja cyber sigurnosti u EU. Druga strategija cyber sigurnosti EU insistira na postojanju „robusnijih i učinkovitijih struktura za promicanje cyber sigurnosti i odgovor na cyber napade u državama članicama ali i u vlastitim institucijama, agencijama i tijelima EU“, što u određenoj mjeri ocrtava doseg područja kibernetičke sigurnosti EU (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku 2017: 3). Slično je važan i poziv na „sveobuhvatniji, višepolitički pristup izgradnji cyber otpornosti i strateške autonomije, sa jakim jedinstvenim tržištem“ koji dobija jači naglasak u odnosu na prvu strategiju EU o kibernetičkoj sigurnosti (Evropska komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku 2017: 3). Druga strategija EU za kibernetičku sigurnost, iako nije pravno obavezujući instrument, također pojašnjava ulogu različitih agencija EU koje oblikuju područje politike kibernetičke sigurnosti.[20]

[20] S. W. Brenner, B. Jaap Koops, Approaches to Cybercrime Jurisdiction, 4, Journal of High Technology Law, 6–7 (2004).

Literatura

1. Akademska i istraživačka mreža HR – CARNet, Phishing napadi.
2. Appazov, A., Legal Aspects of Cybersecurity, Faculty of Law, University of Copenhagen, Kopenhagen, 2014.
3. Brenner, S. W., Jaap Koops B., Approaches to Cybercrime Jurisdiction, 4, Journal of High Technology Law.
4. Cornish, P., Hughes R., Livingstone D., Cyberspace and the National Security of the United Kingdom, Chatham House, UK, 2009.
5. *Edukator: naučno-stručni i informativni časopis*, Travnik, Univerzitet/Sveučilište „Vitez“, 2016.
6. Gerecke, M., Understanding cybercrime, Phenomena, challenges and legal response, Telecommunication Development Sector, 2012.
7. https://ire.ba/sta-znamo-o-cyber-kriminalu/
8. https://mup.ks.gov.ba/kampanja/zastitimo-se-od-cyber-kriminala
9. https://www.sergije-stanic.me/images/Racunarski_virusi2014-2015.pdf
10. James, L., Phishing exposed, Secure Science Corporation, USA, 2005.
11. Kovacs, L., Cyber security policy and strategy in the European Union and Nato, National University of Public Service, Budapest, Hungary, 2018.
12. Markovinović, E., Peer to peer mreže, završni rad, Sveučilište J. J. Strossmayera, Osijek, 2015.
13. Tamarkin, E., Cybercrime, Institute for Security studies, USA, 2014.