Msr Petar Đukić*
Doktorand na Fakultetu bezbednosti
Univerziteta u Beogradu

Pregledni rad
Primljeno: 25. januar 2023.
Prihvaćeno: 4. avgust 2023.
UDK: 343.533::004.738
https://doi.org/10.47152/rkkp.61.2.3

PRAVNI OKVIR ZAŠTITE OD VISOKOTEHNOLOŠKOG KRIMINALA U BOSNI I HERCEGOVINI – analiza strateških ciljeva i mogućnost usklađivanja sa evropskom strategijom sajber bezbednosti

Tema ovog rada jeste pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini, uz analizu strateških ciljeva i mogućnosti usklađivanja sa Strategijom sajber bezbednosti EU za digitalnu deceniju, koja je usvojena pretprošle godine. U radu je dato pojmovno određenje visokotehnološkog kriminala i sajber bezbednosti, kao i njihove osnovne karakteristike. Zatim je, u kratkim crtama, analiziran pravni okvir zaštite od visokotehnološkog kriminala u BiH. Kada je u pitanju Strategija sajber bezbednosti EU za digitalnu deceniju, u nastavku rada su interpretirani njeni najznačajniji delovi, posebno oni koji bi mogli imati aplikativni značaj za Bosnu i Hercegovinu. Na osnovu navedenog, u zaključnim razmatranjima su date odgovarajuće preporuke za unapređenje pravnog i strateškog okvira sajber bezbednosti u BiH.

Ključne reči: visokotehnološki kriminal, sajber bezbednost, zaštita, strategija, pravni okvir, BiH, Evropska unija.

* E-mail: petar.djukic96@yahoo.com

1. Uvod

Bezbednosne dinamike koje su, u nekom (sada već davnom) prošlom vremenu, ispunjavale samo realni prostor, odavno su preplavile i tzv. sajber sferu. Za izmenu bezbednosne paradigme na ovom polju usko se vežu promene životnih stilova i navika ljudi, ali i izuzetan napredak u sferi nauke i tehnologije. Veliki deo svakodnevnih životnih interakcija preseljen je u virtualni (sajber) prostor. Pomenućemo samo činjenicu da je „rad od kuće“[11] sve popularniji (pogotovo nakon pandemije koronavirusa) i pretenduje da preraste u trajniji obrazac. Inače, gde god ljudi obavljaju svoje aktivnosti i gde god stupaju u interesne interakcije sa drugim ljudima, može se očekivati i činjenje nedozvoljenih radnji, pa i krivičnih dela na štetu drugih. To svakako važi i za države. Dakle, bezbednosni rizici koji se ispoljavaju u sajber svetu su veoma heterogeni i kreću se od vršenja krivičnih dela na štetu pojedinaca i pravnih lica preko ili uz pomoć računarskih sistema i mreža do sajber operacija kojima se ugrožava bezbednost država i međunarodnih organizacija kroz sprovođenje akata terorizma ili čak agresije (Milošević, Putnik, 2017: 178).

Visokotehnološki kriminal pokriva širok dijapazon krivičnih dela čiji se broj konstantno povećava, a organizovani kriminal u vezi sa nekim od krivičnih dela iz domena visokotehnološkog kriminala je sve češća pojava. Prema shvatanjima S. Brenner (2002), u virtualnom svetu snaga ne igra nikakvu ulogu i pojedinac koji raspolaže određenim znanjem i tehnologijom može sam učiniti istu štetu koju bi učinilo više ljudi koji rade zajedno kao organizovana grupa. Međutim, kada ciljevi kriminalaca postanu kompleksniji, kada je potrebno izvršiti simultane upade, napade ili druge radnje prema više pojedinaca, kompanija ili država, udruživanje snage, u smislu organizovanog kriminala, opet postaje aktuelno. Isti slučaj je i sa organizovanim (sajber) terorizmom. U kontekstu navedenog, osnovni preduslov borbe protiv visokotehnološkog kriminala jeste funkcionalan strateški i pravni okvir, kako na međunarodnom, tako i na nacionalnom nivou. Takav okvir predstavlja izuzetno dinamičnu kategoriju zbog ubrzanih promena koje se dešavaju na polju razvoja kompjuterske tehnologije. Zakonodavac mora biti svestan tih promena i, u skladu sa prethodno usvojenom strategijom, menjati i dopunjavati pozitivne pravne propise. Inertnost zakonodavaca po ovom pitanju može imati teže posledice nego u bilo kojoj drugoj oblasti (Bejatović, 2012: 21). Budući da tzv. „sajber dobra“ pojedinaca i država predstavljaju stratešku vrednost,

1 Oko 40% Evropljana prešlo je na rad od kuće tokom pandemije koronavirusa, 2020. godine, što je povećalo njihovu ranjivost, ali i ranjivost preduzeća, u odnosu na sajber napade (The EU's Cybersecurity Strategy for the Digital Decade, 2020).

ona bi morala da uživaju i stratešku zaštitu. To bi se najadekvatnije postiglo koncipiranjem i realizovanjem izvesne nacionalne strategije informacione (sajber) bezbednosti, koja bi bila integralna komponenta strategije nacionalne bezbednosti, kao i institucionalizacijom izvesnog podsistema nacionalne bezbednosti koji bi, po principima specijalizacije i profesionalizacije, bio nadležan za njeno sprovođenje (Mijalković i dr., 2010).

U Bosni i Hercegovini, visokotehnološki kriminal je u nivou sa informatizacijom društva, odnosno sa stepenom rasprostranjenosti informacionih tehnologija, ali i međunarodnim refleksijama ove vrste kriminala (Šikman, Milošević, 2012: 4). Predmet našeg interesovanja u ovom radu jeste pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini, uz analizu strateških ciljeva i mogućnosti usklađivanja sa evropskom strategijom sajber bezbednosti – odnosno dokumentom „The EU's Cybersecurity Strategy for the Digital Decade“ (Joint communication to the European Parliament and the Council, Brussels, 16. 12. 2020, JOIN(2020) 18 final). Pri tome, moramo imati u vidu da je Bosna i Hercegovina država specifičnog, složenog ustavno-političkog uređenja, tako da se pravni propisi donose i egzistiraju na četiri nivoa pravne regulative.[22] Ovo u dobroj meri usložnjava i otežava mogućnost sveobuhvatne i detaljne interpretacije pravnog okvira zaštite od ovog oblika kriminala u toj državi. Ipak, kada su u pitanju strateška opredeljenja zemlje, te usvajanje i implementacija međunarodnih standarda (kao npr. evropska strategija sajber bezbednosti), tu glavnu ulogu igraju institucije i organi na državnom nivou, u čijoj nadležnosti je sprovođenje međunarodnih i međuentitetskih krivičnopravnih propisa, te ratifikacija svih međunarodnih dokumenata. U tom smislu, najviše pažnje biće posvećeno sajber bezbednosti na državnom nivou.

2. Pojam sajber bezbednosti i visokotehnološkog kriminala

Pre nego što pređemo na suštinu rada, kratko ćemo se osvrnuti na pojam i neke osnovne karakteristike sajber (informacione) bezbednosti i visokotehnološkog kriminala.

Savremeno poimanje nacionalne, ali i drugih nivoa bezbednosti nezamislivo je bez sektora tzv. informacione ili sajber bezbednosti. Ideja koncepta informacione bezbednosti nije nova, a nastala je krajem 80-ih godina u SAD-u, integrisanjem ranije odvojenih sfera bezbednosti osoblja, kompjuterske bezbednosti, komunikacione bezbednosti i operativne bezbednosti. (Mijalković i dr., 2010:8).

2 Lokalni nivo (Brčko Distrikt Bosne i Hercegovine), kantonalni nivo, entitetski nivo i državni nivo.

Informaciona bezbednost je, dakle, integralna komponenta nacionalne bezbednosti koja podrazumeva stanje zaštićenosti životno važnih vrednosti i interesa pojedinaca, društva i države u informacionoj – sajber sferi od spoljašnjih i unutrašnjih opasnosti (rizika), odnosno stanje zaštićenosti informacione sredine društva koje omogućava njeno formiranje, korišćenje i razvoj u interesu građana, organizacija i države (Petrović, 2007: 10–11).

Jedna od najvećih pretnji po informacionu bezbednost je visokotehnološki kriminal. Na početku treba napomenuti da se, uz izraz „visokotehnološki kriminal“, kao sinonimi koriste i izrazi „kompjuterski kriminal“, „sajber (kiber) kriminal“, „elektronski kriminal“, „internet kriminal“ i drugi. Uz terminološku raznovrsnost, treba ukazati i na raznovrsnost definicija, pri čemu ne postoji neka za koju bismo mogli reći da je opšteprihvaćena. Činjenica je da bi bilo teško jednom definicijom obuhvatiti sve oblike ispoljavanja ovog kriminalnog fenomena, a i pokušaji njegove klasifikacije su, uglavnom, nedostatni. Svoje viđenje visokotehnološkog kriminala davali su razni autori koji su se bavili tom problematikom, ali i međunarodne organizacije u svojim dokumentima, te nacionalni zakonodavci. Ipak, svi se slažu u jednoj stvari, a to je da je u pitanju globalni problem čija ekspanzija može da ugrozi najznačajnije lične, nacionalne, ali i civilizacijske vrednosti.

Prateći razvoj tehnologije, i sama definicija visokotehnološkog kriminala se postepeno razvijala i usložnjavala. Radna grupa eksperata Ujedinjenih nacija je, na Kongresu prevencije kriminala, održanom 2005. godine, u Bangkoku, na Tajlandu, odredila visokotehnološki kriminal kao opšti pojam koji obuhvata krivična dela koja se vrše pomoću kompjuterskog sistema ili mreže, u kompjuterskom sistemu ili mreži ili protiv kompjuterskog sistema ili mreže (United Nations, 2005). U osnovi, sličnu definiciju predstavio je i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala Republike Srbije, u članu 2. – visokotehnološki kriminal podrazumeva „vršenje krivičnih dela gde se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom i elektronskom obliku“. Kako navodi Stephson (2010), visokotehnološki kriminal podrazumeva „svako nezakonito ponašanje vezano za ili u odnosu na kompjuterski sistem i mrežu, uključujući i takav kriminal kakvo je ilegalno posedovanje, nuđenje i distribuiranje informacija preko kompjuterskih sistema i mreža“. Na našim prostorima, definisanjem visokotehnološkog kriminala se, među prvima, bavio prof. dr Đorđe Ignjatović. On koristi sintagmu „kompjuterski kriminalitet“ koji, prema njegovom shvatanju, „predstavlja poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekat krivičnog dela, ukoliko se delo na drugi način ili prema drugom objektu, uopšte ni bi moglo izvršiti ili bi ono imalo bitno

drugačije karakteristike“ (Ignjatović, 1991:142). Naš poznati kriminalista, prof. dr Branislav Simonović (2004: 665) visokotehnološki kriminal definiše kao „društveno opasnu pojavu za čije se ostvarenje učinilac koristi znanjima kompjuterske (informatičke) tehnologije, tako što se kompjuterski sistem shvaćen u najširem smislu (hardver, softver, njihovo jedinstvo; jedan kompjuter ili mreža kompjutera) koristi kao sredstvo ili kao objekt kriminalnog napada ili i jedno i drugo“.

Dakle, sajber kriminal pokriva širok spektar krivičnih dela, uključujući hakovanje kompjutera, podataka i sistema, kompjuterske prevare, te krivična dela vezana za sadržaj, kao što su dečija pornografija i autorska prava (Schreier i dr., 2010: 9). Pobrojati sva ponašanja koja možemo i trebamo podvesti pod pojam visokotehnološkog kriminala nije lak zadatak. Prema listi koju je preporučila grupa eksperata OECD-a, to su:

- neautorizovani pristup, tj. neovlašćeni i protivpravni upad u kompjuterski sistem ili mrežu kršeći mere zaštite (hakovanje);
- neovlašćeno uništenje, brisanje i/ili oštećenje kompjuterskih programa ili podataka,
- računarska sabotaža, u smislu unosa, uništenja, izmene, oštećenja, brisanja, kompjuterskih podataka ili programa sa namerom potkopavanja funkcionisanja kompjuterskih ili telekomunikacionih sistema;
- neovlašćeno sprečavanje i ograničavanje komuniciranja ka kompjuterskom sistemu ili mreži, iz njih i unutar njih;
- kompjuterska špijunaža, u smislu bespravnog otkrivanja, prenošenja ili korišćenja komercijalnih tajni i to sa namjerom da se izazove ekonomski gubitak za lica koja poseduju tu tajnu ili za sebe ili drugog pribavi protivpravna imovinska korist (Organisation for Economic Co-operation and Development, 1986).

Analizom postojećih definicija visokotehnološkog kriminala, možemo izvesti određene zaključke o njegovim karakterističnim obilježjima. U skladu sa potrebama ovog rada, pokušaćemo navesti samo neke osnovne karakteristike visokotehnološkog kriminala:

- raznovrsni oblici ispoljavanja i izražena tendencija pojave novih oblika;
- vidno prisustvo tzv. „tamne brojke“ što znači da veliki broj krivičnih dela ostane neotkriven;
- visokotehnološki kriminal ne poznaje granice između država i kontinenata;
- mogućnost izvršenja krivičnih dela u veoma kratkom vremenskom okviru;
- izvršioci su lica koja u određenoj mjeri poznaju informacione tehnologije;
- anonimnost, zbog koje je mnogo teže otkriti učinioca;
- potencijal za viktimizaciju i štete velikih razmera (Videti: Bošković, Jovičić, 2002: 443–445).

Možemo zaključiti da pojam visokotehnološkog kriminala nije lako definisati, što otežava posao nacionalnim zakonodavcima prilikom koncipiranja krivičnopravnog odgovora. Prema našem mišljenju, uvažavajući i sublimirajući navedene definicije, visokotehnološki kriminal predstavlja skup krivičnih dela koja se čine u sajber prostoru, pri čemu se kompjuterski sistemi, mreže ili podaci javljaju kao sredstvo, objekat ili dokaz izvršenja krivičnog dela. Takođe, uvažavajući činjenicu da izvršioci takvih krivičnih dela nisu sputani nikakvim granicama (pa ni državnim), jer svoje kriminalne akte čine u sajber prostoru, mišljenja smo da ne postoji država koja može potpuno samostalno odgovoriti problemu visokotehnološkog kriminala pa se, zbog toga, mora pridružiti međunarodnoj akciji uz, pre svega, harmonizaciju krivičnih zakona i usklađivanje sa internacionalnim strategijama sajber bezbednosti.

3. Pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini

Pravni okvir zaštite od visokotehnološkog kriminala je sačinjen od odredaba različitih zakona, kojima je bezbednost informaciono-komunikacionih sistema primaran ili sekundaran predmet regulisanja (Milošević, Putnik, 2017:180). Bosna i Hercegovina je država specifičnog ustavno-pravnog uređenja. Naime, činjenica da se BiH sastoji od dva entiteta i jednog distrikta vodi ka zaključku da je podela nadležnosti krucijalna za funkcionisanje ove državne zajednice. Kada su u pitanju krivične stvari i, uopšte, pitanja bezbednosti, sukobi nadležnosti između vlasti na nivou države i entitetskih vlasti česta su pojava. Time se u značajnoj meri podriva efikasnost normativnih i institucionalnih kapaciteta Bosne i Hercegovine u upravljanju savremenim bezbednosnim rizicima u koje svakako spada i visokotehnološki kriminal. U ovom delu rada pokušaćemo, u kratkim crtama, predstaviti pravni okvir zaštite od visokotehnološkog kriminala u BiH.

Institucije države nadležne su, između ostalog, za ratifikaciju međunarodnih dokumenata. U vezi s tim, prvo što trebamo pomenuti jeste to da je Bosna i Hercegovine potpisnica Konvencije o visokotehnološkom kriminalu („Convention on Cybercrime“) – (Službeni glasnik BiH – Međunarodni ugovori, br. 06/2006) koju je Savet Evrope usvojio 23. novembra 2001. godine u Budimpešti. Ratifikacijom ovog značajnog dokumenta u Bosni i Hercegovini su postavljeni temelji za dalju izgradnju pravnog okvira zaštite od visokotehnološkog kriminala.

Sajber bezbednost, kao deo šireg kompleksa nacionalne bezbednosti, trebalo bi da bude obuhvaćena i političko-pravnim dokumentima čiji su predmet nacionalna bezbednost i odbrana (Milošević, Putnik, 2017:186). Međutim, u Bosni

i Hercegovini ne postoji strateški dokument koji bi se odnosio na sajber bezbednost i zaštitu od visokotehnološkog kriminala. BiH, dakle, nije donela svoju strategiju sajber bezbednosti, uprkos obavezama koje joj nalaže proces pristupanja Evropskoj uniji. Naime, Direktiva (EU) 2016/1148 Evropskog parlamenta i Saveta o merama za visoki zajednički nivo bezbednosti mrežnih i informacionih sistema širom Unije[33], između ostalog, nalaže da svaka država članica donosi svoju strategiju za sigurnost informaciono-komunikacionih sistema. U vezi s navedenim, Organizacija za evropsku bezbednost i saradnju je, 2019. godine, pripremila dokument pod nazivom „Smjernice za strateški okvir sajber sigurnosti u Bosni i Hercegovini“.[44]

Zakonodavni mehanizmi za borbu protiv visokotehnološkog kriminala na nivou institucija Bosne i Hercegovine nisu izgrađeni. Razlog tome je što se primarna nadležnost za krivičnopravno suprotstavljanje visokotehnološkom kriminalu nalazi „u rukama“ entiteta i Brčko Distrikta Bosne i Hercegovine, tako da Krivični zakon Bosne i Hercegovine ne propisuje niti jedno krivično djelo koje se neposredno odnosi na ovaj oblik kriminala. Međutim, ukoliko pod pojam visokotehnološkog kriminala podvedemo i krivična dela iz oblasti zloupotrebe autorskih prava, onda moramo pomenuti glavu XXI, pod nazivom „Krivična djela povrede autorskih prava“. Propisano je pet takvih krivičnih dela: Zloupotreba autorskih prava (član 242); Nedozvoljeno korištenje autorskih prava (član 243); Nedozvoljeno korištenje prava proizvođača zvučne snimke (član 244); Nedozvoljeno korištenje prava radiodifuzije (član 245); Nedozvoljena distribucija satelitskog signala (član 246). Dalje, kao dva vrlo bitna zakona koja se posredno odnose na područje sajber bezbednosti u Bosni i Hercegovini možemo navesti Zakon o zaštiti tajnih podataka i Zakon o zaštiti ličnih podataka. Zakonom o zaštiti tajnih podataka uređuju se zajedničke osnove jedinstvenog sistema određivanja, pristupa, korišćenja, čuvanja i zaštite od neovlašćenog otkrivanja, uništavanja i zloupotrebe tajnih podataka iz nadležnosti Bosne i Hercegovine, entiteta i ostalih nivoa državne organizacije Bosne i Hercegovine koji se odnose na javnu bezbednost, odbranu, vanjske poslove ili obaveštajnu i bezbednosnu delatnost, prestanak tajnosti takvih podataka, te postupak bezbednosne provere i izdavanje bezbednosne dozvole za pristup tajnim podacima. Sa druge strane, cilj Zakona o zaštiti ličnih podataka jeste da se na teritoriji Bosne i Hercegovine svim licima, bez obzira na njihovo državljanstvo ili prebivalište, osigura zaštita ljudskih prava i osnovnih sloboda, a naročito pravo na privatnost i zaštitu podataka u pogledu

3 Poznatija kao NIS direktiva: Directive (EU) 2016/1148 of the European Parliament and of the Council – (EU Network and Information Security Directive) of 6 July 2016 Union.

4 Smjernice za strateški okvir sajber sigurnosti u Bosni i Hercegovini. (2019). Sarajevo: OEBS.

obrade ličnih podataka koji se na njih odnose. Jasno nam je koliku ulogu imaju informacioni sistemi i visoke tehnologije u oblasti regulacije ovih propisa, kao i da kršenje njihovih odredba predstavlja ništa drugo do visokotehnološki kriminal. Takođe, sledeći zakonski propisi sa nivoa BiH posredno se odnose na oblast sajber bezbednosti: Zakon o obavještajno-bezbjednosnoj agenciji BiH, Zakon o elektronskom potpisu BiH, Zakon o elektronskom pravnom i poslovnom prometu BiH, Zakon o sprečavanju pranja novca i finansiranju terorizma u BiH, Zakon o komunikacijama BiH, te Zakon o autorskim i srodnim pravima.

Krivično pravo je najvažniji instrument borbe protiv kriminala uopšte, pa tako i visokotehnološkog kriminala. Kao što smo naveli, nadležnost za krivičnopravno suprotstavljanje visokotehnološkom kriminalu pripada entitetima i distriktu. Naravno, taj vid borbe ima dva aspekta – materijalni i procesni.

Krivični zakonik Republike Srpske, u glavi XXXII, pod nazivom „Krivična djela protiv bezbjednosti kompjuterskih podataka“, propisuje sedam krivičnih dela:

1. Oštećenje kompjuterskih podataka i programa (član 407). Ovo krivično delo čini onaj ko neovlašteno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim kompjuterski podatak ili program.
2. Kompjuterska sabotaža (član 408). Radnja ovog krivičnog dela podrazumijeva unošenje, uništenje, brisanje, izmjenu, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim kompjuterski podatak ili program ili uništenje ili oštećenje kompjutera ili drugog uređaja za elektronsku obradu i prenos podataka sa namerom onemogućavanja ili znatnog ometanja postupka elektronske obrade i prenosa podataka koji su od značaja za republičke organe, javne službe, ustanove, privredna društva ili druge subjekte.
3. Izrada i unošenje kompjuterskih virusa (član 409). Krivično delo čini onaj ko napravi računarski virus u nameri njegovog unošenja u tuđi kompjuter ili kompjutersku ili telekomunikacionu mrežu, kao i onaj ko unese računarski virus u tuđi kompjuter ili kompjutersku mrežu i time prouzrokuje štetu.
4. Kompjuterska prevara (član 410). Ovo delo je, zapravo, specifičan oblik klasičnog krivičnog dela prevare i čini ga onaj ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu.
5. Neovlašteni pristup zaštićenom kompjuteru, zaštićenoj mreži, telekomunikacionoj mreži i elektronskoj obradi podataka (član 411). Ovo delo ima tri oblika. Prvi oblik čini onaj ko se, kršeći mere zaštite, neovlašteno uključi u kompjuter ili kompjutersku mrežu ili neovlašteno pristupi elektronskoj

obradi podataka. Drugi oblik inkriminiše snimanje ili upotrebu podatka dobijenog na prethodno opisan način. Trećim oblikom inkriminisana je izrada, pribavljanje, prodaja ili davanje na korištenje uputstva ili sredstva koje je namenjeno za ulaženje u kompjuterski sistem.

6. Sprečavanje i ograničavanje pristupa javnoj kompjuterskoj mreži (član 412). Ovo delo podrazumeva neovlašteno sprečavanje ili ometanje pristupa javnoj kompjuterskoj mreži.
7. Neovlašteno korištenje kompjutera ili kompjuterske mreže (član 413). Ovo delo čini onaj ko neovlašteno koristi kompjuterske usluge ili kompjutersku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist.

Krivični zakon Federacije Bosne i Hercegovine, u glavi XXXII, pod nazivom „Krivična djela protiv sustava elektronske obrade podataka“, propisuje šest krivičnih dela: Oštećenje računalnih podataka i programa (član 393); Računalno krivotvorenje (član 394); Računalna prijevara (član 395); Ometanje rada sustava i mreže elektronske obrade podataka (član 396); Neovlašćeni pristup zaštićenom sustavu i mreži elektronske obrade podataka (član 397); Računalna sabotaža (član 398). Gotovo identične inkriminacije sadrži i Krivični zakon Brčko distrikta Bosne i Hercegovine, u glavi XXXII.

Drugi aspekt krivičnopravne borbe protiv visokotehnološkog kriminala je krivičnoprocesni. Svi zakoni o krivičnom postupku u Bosni i Hercegovini sadrže odredbe procesnopravnog karaktera kojima su predviđeni procesni mehanizmi i ovlašćenja svih učesnika u krivičnom postupku u pogledu otkrivanja učinilaca krivičnih dela, prikupljanja dokaza, procesuiranja i suđenja. Efikasno otkrivanje i suzbijanje visokotehnološkog kriminala uključuje i veoma specifične operativne mere i radnje, kao i posebne dokazne radnje – „specijalne istražne tehnike“ (Urošević i dr., 2012: 35). Treba reći da zakoni o krivičnom postupku u Bosni i Hercegovini ne sadrže nikakva posebna procesna pravila koja bi se isključivo odnosila na visokotehnološki kriminal. S obzirom na ovo, u postupku otkrivanja, dokazivanja i presuđenja krivičnih djela visokotehnološkog kriminala primenjuju se dve vrste odredaba ZKP-a. Prvo, to su odredbe kojima se propisuju posebne istražne radnje. Drugo, tu su odredbe opšteg karaktera koje se odnose na sve vrste krivičnih dela, pa i krivična dela visokotehnološkog kriminala (Bejatović, 2012: 25).

Na kraju, kada je u pitanju BiH, treba reći da jedino Republika Srpska ima regulativu koja tretira oblast sajber bezbednosti. Naime, Zakon o informacionoj bezbjednosti prisutan je od 2011. godine u pravnom sistemu Republike Srpske i svakako je deo pravnog okvira zaštite od visokotehnološkog kriminala. Po svojoj prirodi, nomotehničkom pristupu i strukturi predstavlja jasan, precizan i koncizan organski okvir za uspostavljanje i održavanje informacione bezbednosti, kako u

organima javne uprave Republike Srpske, tako i drugim relevantnim subjektima koji za ovim vidom bezbednosti ispolje potrebu (Vranješ, Rajčević, 2012: 123). Zakon o informacionoj bezbednosti definiše informacionu bezbednost kao bezbednost koja se obezbeđuje primenom mera i standarda informacione bezbednosti ili, preciznije, kao stanje poverljivosti, celovitosti i dostupnosti podataka. Sledstveno navedenoj definiciji, zakon daje određenje i njenih strukturalnih pojmova. Posebnu pažnju zakon posvećuje merama informacione bezbednosti, pri čemu propisuje tri vrste mera: fizičku zaštitu, zaštitu podataka i zaštitu informacionog sistema.

Zbog razrade Zakona o informacionoj bezbjednosti donesena je Uredba o mjerama informacione bezbjednosti (Službeni glasnik Republike Srpske, br. 91/12). Ovom Uredbom utvrđuju se mere informacione bezbednosti kojima se obezbeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou, tj. bliže se razrađuju Zakonom propisane mere zaštite.

Mere fizičke zaštite sprovode se radi sprečavanja neovlašćenog ili nasilnog ulaska lica u objekte i prostorije u kojima se nalaze podaci odnosno uređaji sa podacima, sprečavanja i otkrivanja zloupotreba podataka od strane zaposlenih, kao i otkrivanja i reagovanja na rizike.

U pogledu zaštite podataka, uredbom je uređeno da računar za vođenje baze podataka i centralni računar informacionog sistema (server) moraju biti opremljeni: sistemom za bezbedno prijavljivanje za rad sa mogućnošću evidentiranja ostvarenih pristupa, kako bi se pristup serveru mogao kontrolisati i ograničiti; mehanizmom za sprečavanje neovlašćenog iznošenja i unošenja podataka upotrebom prenosivih informatičkih medija, komunikacionih priključaka i priključaka za ispis podataka i mehanizmom zaštite od računarskih virusa i drugih štetnih programa. Pored navedenog, pristup bazi podataka dozvoljen je samo licima zaduženim za održavanje i razvoj informacionog sistema, dok je pristup telekomunikacionom, računarskom i aplikativnom sistemu za obradu podataka dozvoljen uz upotrebu odgovarajućeg korisničkog imena i pripadajuće lozinke.

Najzad, korisničko ime i pripadajuća lozinka ne smeju se otkriti i dati na upotrebu drugom licu.

Zaštita informacionih sistema nalaže da računar za vođenje baze podataka, server i računarsku mrežu postavlja i ugrađuje stručno lice, u skladu sa projektnom dokumentacijom, važećim normama, standardima i tehničkim uputstvima.

Pored navedenih mera informacione bezbednosti, pomenuta uredba razrađuje i upravljanje rizikom informacione bezbednosti što podrazumeva planiranje, organizovanje i usmeravanje aktivnosti radi obezbeđivanja uslova da rizici ne ugroze neprekidno funkcionisanje, odnosno poslovanje organa, pravnih i fizičkih lica.

Treba reći i da Zakon o informacionoj bezbjednosti propisuje i da se mere informacione bezbednosti sprovode se u skladu sa standardima informacione

bezbednosti. Minimalni standardi informacione bezbednosti kojima se obezbeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou utvrđeni su Pravilnikom o standardima informacione bezbjednosti. Ovaj podzakonski akt donesen je od strane ministra nauke i tehnologije (broj: 19/6-010-/91-23/12 od 10. 5. 2013.) i, ako smo za Uredbu rekli da razrađuje Zakon, onda slobodno možemo reći da Pravilnik o standardima informacione bezbjednosti dalje razrađuje Uredbu o mjerama informacione bezbjednosti. Dakle, Pravilnikom je precizno definisano postupanje odgovornih lica u sprovođenju mera informacione bezbednosti.

Ova tri navedena propisa – zakon, uredba i pravilnik su od velikog značaja i za primenu krivičnog prava. Videli smo da određen broj krivičnih dela visokotehnološkog kriminala predstavlja krivična dela blanketnog karaktera čije biće upućuje na primenu ovih propisa. Npr. videli smo da neke inkriminacije sadrže odrednice kao što su: „ko kršeći mjere zaštite“ ili „ko neovlašteno“. Te mere zaštite i ta ovlaštenja upravo propisuju propisi koje smo interpretirali u ovom odeljku.

Takođe, ovim propisima uspostavljeno je i Odjeljenje za informacionu bezbjednost Republike Srpske („CERT“). Radi se o posebnoj organizacionoj jedinici za delovanje u hitnim slučajevima, čiji je zadatak koordinacija prevencije i zaštite od računarskih bezbednosnih incidenata na internetu i drugih rizika bezbednosti informacionih sistema organa i drugih fizičkih i pravnih lica.

Ono što je interesantno jeste da Federacija Bosne i Hercegovine još uvek nema propis koji bi bio pandan Zakonu o informacionoj bezbjednosti Republike Srpske. Ipak, Vlada Federacije je, dana 8. 10. 2020. godine, na svoj zvaničnom internet sajtu, objavila Poziv za dostavljanje primedbi, predloga i komentara na Zakon o informacionoj sigurnosti i sigurnosti mrežnih i informacionih sistema[55]. Tada je ovaj propis bio u fazi podnacrta, a njegova „sudbina“ danas, dve godine kasnije, nije poznata.

4. Strategija sajber bezbednosti Evropske unije – aplikativni aspekt

U martu 2021. godine, na predlog Evropske komisije, Savet Evrope usvojio je dokument pod nazivom „Strategija sajber bezbednosti EU za digitalnu deceniju“[66] (u daljem tekstu: Strategija). Ovaj strateški dokument predstavlja odgovor

5 https://fmpik.gov.ba/bh/aktuelnosti/obavje%C5%A1tenja/308-poziv-za-dostavljanje-primjedbi,-prijedloga-i-komantara-na-zakon-o-informacionoj-sigurnosti-i-sigurnosti-mre%C5%BEnih-i-informacionih-sistema.html

6 “The EU’s Cybersecurity Strategy for the Digital Decade”, Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint communication to the European Parliament and the Council, Brussels, 16.12.2020, JOIN(2020) 18 final.

Evropske unije na ubrzanu digitalizaciju i povećano oslanjanje na nove informacione tehnologije – trendove koje je kriza izazvana koronavirusom učinila očiglednim (Novičić, 2021). Kako navodi Tasheva (2021), ogromna digitalna tranzicija postavila je izazove sajber bezbednosti na tri fronta: previše novih korisnika je na mreži, digitalizacija malih i srednjih preduzeća i javnih usluga je bila prebrza, a nivo sajber otpornosti kritične infrastrukture ostao je prenizak. Zbog svega navedenog, Unija je morala pružiti novi i sveobuhvatan odgovor, u vidu Strategije. U skladu sa temom i potrebama ovog rada, osvrnućemo se na one delove Strategije koji se eksplicitno odnosne na visokotehnološki kriminal, odnosno one delove sa kojima je moguće i potrebno uskladiti strateško-pravni okvir zaštite od ovog vida kriminala u BiH.

Prvi deo Strategije je uvodni i deskriptivnog je karaktera. U ovom delu, sajber bezbednost je prepoznata kao integralni deo „bezbednosti Evropljana“, te se navodi da je ista od suštinskog značaja za izgradnju otporne, „zelene“ i digitalne Evrope. Posebno je apostrofirana zavisnost kritične infrastrukture (transport, energetika, zdravstvo, telekomunikacije, finansije) od bezbednosti mrežnih i informacionih sistema. Takođe, upozorava se na tzv. hibridna dejstva u sajber prostoru, odnosno rat (dez)informacijama koji podriva međunarodnu bezbednost. Ukazano je i na činjenicu da istrage gotovo svih vrsta krivičnih dela imaju digitalnu komponentu. Unapređenje sajber bezbednosti je, stoga, od suštinskog značaja za poverenje ljudi u inovacije, povezanost i automatizaciju, kao i za zaštitu osnovnih prava i sloboda, uključujući prava na privatnost i zaštitu ličnih podataka, kao i slobodu izražavanja. Uvažavajući napredak postignut po prethodnim strategijama, Strategija sadrži konkretne predloge za primenu tri glavna instrumenta – regulatornih, investicionih i političkih instrumenata – za rešavanje tri oblasti delovanja EU – (1) otpornost, tehnološki suverenitet i liderstvo, (2) izgradnja operativnih kapaciteta za sprečavanje, odvraćanje i reagovanje, i (3) unapređenje globalnog i otvorenog sajber prostora. Kao što smo rekli, u nastavku rada biće prezentovani pojedini – najpraktičniji delovi Strategije koje bi bilo potrebno implementirati u BiH, zemlju koja pretenduje da postane član EU.

Prvo, Strategija predlaže reviziju zakonodavstva o kritičnoj infrastrukturi – energija, transport, zdravstvo. Kao cilj je proklamovano smanjenje nedoslednosti na unutrašnjem tržištu, poboljšanje izveštavanja o bezbednosti i incidentima, nacionalnog nadzora, kao i kapaciteta nadležnih tela (Novičić, 2021). Takođe, pominje se i jačanje „sajber otpornosti“ demokratskih procesa i institucija, sa posebnim akcentom na slobodne izbore, demokratski diskurs i medijski pluralitet. Mišljenja smo da je ovaj deo Strategije posebno značajan za zemlje kandidate za članstvo u EU, kao što je BiH. U ovoj zemlji nije uspostavljen jedinstven sistem zaštite kritične infrastrukture, a pitanja sprovođenja slobodnih izbora i medijskih sloboda uvek

su u žiži interesovanja domaće i evropske javnosti. Nikako ne treba prenebregnuti uticaj koji događaji i delovanja u sajber prostoru imaju na kritičnu infrastrukturu, ali i na implementaciju demokratskih procesa, a što je Strategija i prepoznala.

Drugo, Strategija govori o izgradnji tzv. „evropskog sajber štita“. Zapravo, reč je o mreži bezbednosnih operativnih centara zaduženih za prepoznavanje i prijavljivanje sajber pretnji i sajber napada, te periodičnog sumiranja (kroz izveštaje) stanja sajber bezbednosti na nivou EU. Razmenjujući informacije i prevenirajući sajber napade, ovaki centri bi značajno doprineli sajber bezbednosti Evrope, kreirajući svojevrstan sajber štit iznad „evropskog neba“. U tom smislu, Evropska agencija za sajber bezbednost će pružati podršku izgradnji nacionalnih operativnih centara, pre svega u smislu finansiranja[77] i obuke osoblja. Prema našem mišljenju, posebno je značajno što bi ovi centri pomagali nacionalnim pravosudnim i policijskim organima u borbi protiv visokotehnološkog kriminala, praktično im dostavljajući dokaze koji bi se mogli koristiti u krivičnom postupku.

Treće, dokument govori i o bezbednosti tzv. „internet stvari“. Radi se o uređajima povezanim na internet, na način koji im omogućuje da razmenjuju podatke i bez direktnog učešća čoveka, a broj tih uređaja već sada premašuje broj ljudi na Zemlji (Novičić, 2021). Zbog potencijalno štetnih posledica masovne upotrebe ovih uređaja, bitno je voditi računa o njihovoj bezbednosti, a da se, pri tom, ne naruše njihove performanse. Evropska komisija već preduzima mere u pravcu kreiranja šema sertifikacije ovakvih uređaja. Takva pravila uključuju različite obaveze za proizvođače internet stvari, npr. da se bave ranjivostima softvera, kao i da obezbede, na kraju životnog veka uređaja, brisanje ličnih i drugih osetljivih podataka korisnika. Mišljenja smo da edukacija građana o bezbednom korišćenju „internet stvari“ predstavlja važan činilac sajber bezbednosti evropskog prostora. Pored toga, sve „internet stvari“ i druga tehnologija koja ima poreklo van evropskog tržišta, predstavljaju dodatnu opasnost, jer su nepoznanica i za evropske stručnjake. Tako Farrand i Carrapico (2022), govore o potrebi potpunog vraćanja tzv. „digitalnog suvereniteta“ Evropske unije. Naime, EU je shvatila da njeno prekomerno oslanjanje na tehnologiju u stranom vlasništvu ili tehnologiju koja potiče od privatnih aktera iz SAD i Kine, samo po sebi predstavlja pretnju sajber bezbednosti.

Četvrto, a nastavno na gore navedeno, jedan od ciljeva Strategije jeste i pojačano prisustvo evropskih firmi u lancima nabavke tehnologije, uključujući obećavajuću ulogu Evropskog centra za industriju, tehnologiju i istraživanje u oblasti sajber bezbednosti, kojim upravlja EU, zajedno sa državama članicama

7 U dokumentu je pomenut budžet od preko 300 miliona eura za potrebe podrške jačanju javno-privatnog partnerstva i prekogranične saradnje u sajber bezbednosti, kao i za potrebe usavršavanja postojećih i izgradnje novih operativnih centara.

(Novičić, 2021; Pruckova, 2021). Potrebno je da Evropska unija uspostavi punu kontrolu nad svojom digitalnom infrastrukturom i tehnološkom proizvodnjom. U tom cilju, planirana je pomoć za „bezbednu digitalnu transformaciju“, odnosno lanac nabavke koji uključuje tehnologiju naredne generacije procesora, ultra bezbedno povezivanje na internet, kao i 6G mrežu. U fokusu navedenog je podsticanje privatnih investicija, javno-privatnog partnerstva, kao i podrška malim i srednjim preduzećima. Cilj je i da se države podstaknu na ulaganje u industriju tehnologija. Predviđena je i podrška za razvoj namenskih programa edukacije za sajber bezbednost (pominje se i razvijanje programa master akademskih studija), istraživanje i internet inovacije koje razvijaju tehnologije za poboljšanje privatnosti i bezbednu komunikaciju. Sprovođenje ovih inicijativa, u okviru agende EU o digitalnom suverenitetu, posebno će zahtevati „dalje širenje postojećih javno-privatnih partnerstava, posebno u oblastima brzih tehnoloških promena, kao što su robotika, veštačka inteligencija, kvantno računarstvo...“ (Farrand, Carrapico, 2022: 450).

Peto, Strategija se referiše i na radnu snagu koja ima veštine u pogledu sajber bezbednosti. Naime, procene govore da postoji 291.000 slobodnih radnih mesta za stručnjake te vrste u Evropi. U tom smislu, napori EU da unapredi radnu snagu, da razvije, privuče i zadrži najbolje talente za sajber bezbednost i da ulaže u istraživanje i inovacije svetske klase, čine važnu komponentu opšte zaštite od sajber pretnji. Ovo polje nudi veliki potencijal. Potrebno je raditi na podizanju svesti o sajber bezbednosti među pojedincima, posebno decom i mladima, kao i organizacijama, a posebno malim i srednjim preduzećima. Mišljenja smo da je, pored navedenog, potrebno raditi i na planu stvaranja visokoobrazovanih stručnjaka za sajber bezbednost. U tom kontekstu, primera radi, Blažič J. B. (2022: 3032) navodi da se odgovori na nedostatak veština u oblasti sajber bezbednosti mogu naći u „obogaćivanju nastavnih planova i programa visokoškolskih ustanova novim sadržajima iz oblasti koje su najmanje obuhvaćene, kao što su organizacioni ili ljudski aspekti sajber bezbednosti“. Autorka navodi da primeri dobre prakse postoje u najrazvijenijim zemljama EU, ali i da je njihov broj veoma mali, te da je potrebna politička volja za iznalaženje zajedničkih šema akreditacije studijskih programa.

Šesto, kao važan korak ka uspostavljanju evropskog okvira za upravljanje krizama sajber bezbednosti, predstavljena je ideja o „Zajedničkoj sajber jedinici“, kao svojevrsnoj virtualnoj i fizičkoj platformi za saradnju različitih zajednica sajber bezbednosti u EU. Jedinica bi mogla da popuni dve glavne praznine koje, trenutno, povećavaju ranjivost i stvaraju neefikasnost po pitanju odgovora na prekogranične pretnje i incidente koji utiču na Uniju. Prvo, civilne, diplomatske, bezbednosne i odbrambene sajber-bezbednosne zajednice još uvek nemaju

zajednički prostor za negovanje strukturisane operativne i tehničke saradnje. Drugo, relevantni akteri u oblasti sajber bezbednosti još uvek nisu u mogućnosti da iskoriste puni potencijal operativne saradnje i međusobne pomoći u okviru postojećih mreža i zajednica. Ovo uključuje odsustvo platforme koja omogućava operativnu saradnju sa privatnim sektorom. Jedinica treba da poboljša i ubrza koordinaciju i omogući EU da se suoči i odgovori na sajber incidente i krize velikih razmera. Ona ne bi bila dodatno, samostalno telo, niti bi uticala na nadležnosti i ovlašćenja nacionalnih organa bezbednosti. Umesto toga, Jedinica bi delovala kao zaštitni mehanizam i virtualna platforma u kojoj nacionalne države mogu da se oslanjaju na međusobnu podršku i stručnost. Takođe, uspostavljanje Jedinice bi uticalo na ispunjenje tri glavna cilja. Prvo, to bi osiguralo spremnost svih zajednica za sajber bezbednost; drugo, kroz razmenu informacija obezbedilo bi kontinuiranu zajedničku svest o stanju sajber bezbednosti; treće, to bi ojačalo koordiniran odgovor i oporavak (Pruckova, 2021). Još jednom naglašavamo da je regionalna bezbednosna saradnja u borbi protiv visokotehnološkog kriminala uslov bez kojeg se ne može.

Sedmo, jedno manje poglavlje u okviru Strategije odnosi se na zaštitu od visokotehnološkog kriminala. Napomenuto je da istrage gotovo svih vrsta krivičnih dela imaju svoju digitalnu komponentu, a efektivna i efikasna zaštita od visokotehnološkog kriminala je ključni faktor u ostvarivanju sajber bezbednosti – nije dovoljno samo biti otporan, potrebno je identifikovati i procesuirati sajber kriminalce. U tom kontekstu, Evropska komisija najavljuje da će nastaviti „sveobuhvatan pristup“ saradnji raznih aktera sajber bezbednosti i (kao što je npr. Europol), da će dalje organizovati zajedničke konferencije, formulisati izveštaje itd. (Novičić, 2021). U vezi s tim, EU i nacionalne vlasti treba da prošire i unaprede istražne kapacitete organa za sprovođenje zakona po pitanju visokotehnološkog kriminala, u potpunosti poštujući osnovna ljudska prava i slobode, te uspostavljajući ravnotežu između slobode i sajber bezbednosti. Takođe, EU bi trebalo da bude u stanju da se uhvati u koštac sa sajber kriminalom kroz svrsishodno i potpuno primenjeno zakonodavstvo. U tom kontekstu, govori se i o evidentnoj zastarelosti postojeće regulative Unije o visokotehnološkom kriminalu, koja ne pruža najbolji mogući okvir nacionalnim zakonodavcima (Fahey, 2022). Međutim, regulativu mora pratiti i osposobljavanje relevantnih institucija, pre svega policijskih organa. Organi za sprovođenje zakona moraju biti potpuno opremljeni za digitalne istrage, uz neophodne veštine i forenzičke alate. Pored toga, Europol će dalje razvijati svoju ulogu stručnog centra za podršku nacionalnim organima za sprovođenje zakona u borbi protiv „sajber omogućenog“ i „sajber zavisnog“ kriminala, doprinoseći definisanju zajedničkih forenzičkih standarda. Komisija je najavila i nastavak rada na obezbeđenju kanala za dobijanje

prekograničnog pristupa elektronskim dokazima za potrebe kriminalističkih istraga, uz poštovanje svih zaštitnih mera.

Osmo, Strategija promoviše tzv. diplomatski paket alata za sajber bezbednost, koji EU koristi da spreči, obeshrabri, odvrati i odgovori na zlonamerne sajber aktivnosti . U kontekstu toga, EU će podsticati uspostavljanje Radne obaveštajne grupe za sajber bezbednost, sastavljene od predstavnika zemalja članica, radi unapređenja strateške obaveštajne saradnje o sajber pretnjama i aktivnostima. U ovaj proces biće uključena sva tela koja se bave obaveštajnim radom, suzbijanjem dezinformacija i hibridnog stranog uticaja, razvojem situacione svesti i sl. To bi doprinelo odgovornom ponašanju država i saradnji u sajber prostoru, pogotovo u borbi protiv najtežih sajber pretnji koje ugrožavaju kritičnu infrastrukturu, demokratske institucije i procese, lance snabdevanja, intelektualnu svojinu i dr. Ako se zemlje članice EU okrenu istinskoj sajber diplomatiji, vođenoj maksimom „strateške otvorenosti“ u svojoj institucionalnoj, demokratskoj i ekonomskoj dimenziji, one mogu obezbediti da posleratna era prosto ne postane „digitalna predratna era“ (Bendiek, Kettemann, 2021: 7). Bez dalje elaboracije, sugerisana je i mogućnost da se Paket alata sagleda u kontekstu upotrebe ugovornih klauzula o uzajamnoj odbrani i solidarnosti koje pokrivaju čitav spektar scenarija koji mogu zahtevati od država članica da obezbede uzajamnu pomoć u slučaju sajber napada, ali odluka o vrsti pomoći ostavljena je državama članicama (Novičić, 2021).

Da zaključimo, možemo reći da je rat u Ukrajini samo vrh ledenog brega onoga što doživljavamo unutar globalnog bezbednosnog okruženja, koje postaje sve kompleksnije i međuzavisnije. Sajber otpornost Evropske unije, njenih članica, ali i zemalja koje pretenduju da postanu članice, ugroženija je nego ikada pre. Sajber napadi i hibridne pretnje su, nažalost, deo svakodnevice za evropsku bezbednosnu arhitekturu. Stoga, sveobuhvatan pristup EU zasnovan na poverenju, solidarnosti i uzajamnoj pomoći je ključan za borbu protiv sadašnjih i budućih pretnji. Predstavljena Strategija predstavlja veliki iskorak ka tom cilju. Javno-privatno partnerstvo, jedinstveni lanci snabdevanja, mere zaštite, koordinisana borba protiv visokotehnološkog kriminala, formiranje zajedničkih istražnih timova, samo su neki od delova dokumenta koji mogu značajno doprineti bezbednosti Unije, ali i onih zemalja koji teže da postanu njeni punopravni članovi. U tom pogledu, kada je u pitanju izgradnja i jačanje sajber kapaciteta, EU će ostati fokusirana na Zapadni Balkan. Njeni napori, u tom pravcu, treba da podrže razvoj zakonodavstva i politika zapadnobalkanskih zemalja (uključujući BiH), u skladu sa relevantnim politikama i standardima EU sajber diplomatije. EU takođe treba da pomogne ovim zemljama u suočavanju sa rastućim izazovima zlonamernih sajber aktivnosti koje direktno štete razvoju njihovih društava i integritetu i bezbednosti demokratskih sistema i procesa.

5. Zaključna razmatranja

Sajber prostor nudi široke mogućnosti za razvoj bosanskohercegovačke ekonomije, kao i za sve građane BiH, budući da broj aktivnih korisnika interneta i broj konektovanih uređaja u ovoj zemlji eksponencijalno raste. Zbog toga Bosna i Hercegovina mora unaprediti svoje kapacitete (pre svega pravne) za suzbijanje sajber pretnji, a posebno visokotehnološkog kriminala. Ovaj cilj najlakše će postići uplivom u međunarodne i regionalne tokove saradnje u ovoj oblasti. U kontekstu toga, jedan od uslova koji Bosna i Hercegovina mora ispuniti na svom putu ka članstvu u EU svakako je i adekvatan nivo sajber bezbednosti. Obaveza BiH, u tom smislu, jeste i donošenje adekvatne strategije sajber bezbednosti. To se do danas nije dogodilo, a potrebno je što pre, ne samo radi pukog udovoljavanja evropskim birokratama, već zbog jedne realne potrebe.

Pravni okvir zaštite od visokotehnološkog kriminala u Bosni i Hercegovini moramo posmatrati kroz prizmu ustavno-političkog ustrojstva državne zajednice. Dakle, razlikujemo državne i entitetske pravne mehanizme za suprotstavljanje ovom obliku kriminala. Ovde bismo, takođe, trebali naglasiti sve probleme uzrokovane složenošću sistema bezbednosti Bosne i Hercegovine i relativno čestim sukobima nadležnosti između institucija različitih nivoa vlasti. To svakako utiče na efikasnost represivnog aparata u BiH da odgovori izazovima koje nameću novi oblici kriminala koji ne poznaju ni državne granice, a kamoli kantonalne ili entitetske linije razgraničenja. Takođe, različiti nivoi vlasti imaju različite nivoe pripremljenosti, koji su doveli do različitog pristupa pitanjima sajber bezbednosti u okviru Bosne i Hercegovine. Rezultat je nejednak nivo zaštite korisnika, kako u javnom, tako i u privatnom sektoru, a koji podriva ukupni nivo zaštite sajber prostora, te onemogućava pravovremeno delovanje, saradnju i koordinaciju sa ostalim državama u regiji i svetu (OEBS, 2019).

Bosna i Hercegovina potpisnica je Konvencije o visokotehnološkom kriminalu iz 2001. godine što je svakako bio najvažniji korak ka uspostavljanju adekvatnog pravnog okvira zaštite od ovog kriminalnog fenomena. Ipak, BiH treba dalje raditi na planu usvajanja nove i usaglašavanja postojeće (zakonske i podzakonske) legislative, prvenstveno sa aktima Evropske unije, uključujući i gore opisanu Strategiju, kao i drugim međunarodnim propisima, obavezama i standardima sajber bezbednosti. Neusklađenosti treba utvrditi i, gde je moguće, otkloniti. Ono što je svakako potrebno jeste, u Krivičnom zakonu BiH, propisati krivična dela iz domena visokotehnološkog kriminala, sa međunarodnim i međuentitetskim elementima. Međutim, puka harmonizacija prava BiH sa odgovarajućim međunarodnim standardima će ostati prosto ispunjavanje forme ukoliko se ne preduzmu konkretni potezi za usaglašavanje društvene i normativne stvarnosti. U svetlu

toga, potrebno je raditi na podizanju nivoa svesti i znanja o sajber sigurnosti, jačati obrazovne pogone na tom planu (specijalističke ili master akademske studije), te stimulisati naučna istraživanja.

Republika Srpska ima dosta upotpunjene zakonske i podzakonske mehanizme za zaštitu od visokotehnološkog kriminala. U ovom entitetu uspostavljeni su pravni, ali i institucionalni kapaciteti koji su, u zadovoljavajućoj meri, usklađeni sa evropskim zahtevima koji, kako mnogi navode, prednjače u odnosu na Federaciju Bosne i Hercegovine, ali i na neke zemlje okruženja. Krivični zakonik Republike Srpske, donesen pre svega pet godina, sadrži inkriminacije koje odgovaraju trendovima visokotehnološkog kriminala u Bosni i Hercegovini. Takođe, veoma značajan pravni akt u ovom smislu je i Zakon o informacionoj bezbjednosti Republike Srpske, ali i podzakonski akti koji ga dalje razrađuju. Ovim propisima uspostavljeno je Odjeljenje za informacionu bezbjednost Republike Srpske („CERT“). Možemo zaključiti da je sličan zakon potrebno doneti i u Federaciji Bosne i Hercegovine.

Na kraju, ukratko ćemo analizirati šta bi to BiH mogla uraditi na planu usklađivanja sa Strategijom sajber bezbednosti EU za digitalnu deceniju.

Prvo, Bosna i Hercegovina mora revidirati zakonodavstvo o kritičnoj infrastrukturi. Za sada, samo Republika Srpska ima usvojen zakon o kritičnoj infrastrukturi. Takav zakon je potrebno doneti i u Federaciji Bosne i Hercegovine, kao i na državnom nivou, za oblasti iz nadležnosti države. Ovim zakonima treba da bude propisana zaštita informaciono-komunikacionih sistema za pružanje ključnih usluga, odnosno definisana kritična informaciono-komunikaciona struktura (elektronske komunikacije, prenos podataka, informacioni sistemi, pružanje audio, i audio i video medijskih usluga), kako je to već učinjeno na nivou Republike Srpske. Po tom pitanju, potrebno je i zakonski definisati obavezu provođenja zaštite javne informaciono-komunikacione infrastrukture za sve javne i privatne operatore.

Drugo, Bosna i Hercegovina je jedina zemlja u Evropi koja nema uspostavljen CSIRT sistem – sistem pomoći korisnicima interneta u primeni proaktivnih mera za smanjivanje rizika od sajber incidenata te pružanje pomoći u suzbijanju posledica nastalih sajber incidenata. Ovaj sistem je potrebno hitno uspostaviti na nivou BiH, kako bi država postala deo tzv. evropskog sajber štita.

Treće, u Bosni i Hercegovini je neophodno uspostaviti sistem sertifikacije tzv. internet stvari, odnosno odgovarajuće obaveze za proizvođače takvih uređaja (da se bave ranjivostima softvera, kao i da obezbede, na kraju životnog veka uređaja, brisanje ličnih i drugih osetljivih podataka korisnika...).

Četvrto, Bosna i Hercegovina treba da bude uključena u evropski lanac nabavke tehnologija, odnosno investirati u nove tehnologije po principu javno-privatnog partnerstva – sa preduzećima i korporacijama koje razvijaju i nude proizvode,

rešenja i usluge iz domena sajber bezbednosti, kao i sa operatorima ključnih usluga. Na ovaj način država bi bila zaštićena od neproverenih tehnologija poreklom iz vanevropskih tržišta i koje, kako smo i videli, mogu da ugrize sajber bezbednost Unije.

Peto, Bosna i Hercegovina mora ulagati u ljudske resurse – radnu snagu koja raspolaže veštinama i znanjima iz oblasti sajber bezbednosti. Cilj je da razvije, privuče i zadrži najbolje talente za sajber bezbednost i da ulaže u istraživanje i inovacije. Takođe, univerziteti u Bosni i Hercegovini moraju preduzeti aktivnosti na planu akreditacije studijskih programa za stvaranje visokoobrazovanih stručnjaka za sajber bezbednost.

Šesto, Bosna i Hercegovina se mora aktivno uključiti u sve tokove saradnje po pitanju sajber bezbednosti – međunarodna, a pre svega regionalna saradnja. Ova saradnja obuhvata razmenu informacija o izazovima, rizicima i pretnjama sajber bezbednosti, unutar tzv. Zajedničke sajber jedinice, koja bi trebala da bude potpuno opremljena (u tehničkom i operativnom smislu) do juna 2023. godine.[88]

Sedmo, neophodno je dalje usavršavanje, pre svega, operativno-istražnih kapaciteta za zaštitu od visokotehnološkog kriminala. Primera radi, bitan nedostatak važećih zakona o krivičnom postupku u BiH (ima ih četiri) jeste što ne nude definiciju dokaza, a samim tim ni definiciju elektronskog dokaza, čija specifičnost proizilazi iz njihove prirode (vrlo lako se mogu izmeniti ili uništiti, mogu biti smešteni na udaljenom serveru van teritorijalne nadležnosti organa koji ih prikupljaju, mogu biti vidljivi ili nevidljivi). Zakoni o krivičnom postupku u BiH ne predviđaju posebne mehanizme i ovlašćenja procesnih subjekata u pogledu rada s ovom vrstom dokaza, već se primenjuju opšta procesna pravila, kao i pogledu svih ostalih dokaza. Ovo je neophodno izmeniti unošenjem posebnih procesnih normi o elektronskim dokazima. Paralelno s tim, potrebno je unaprediti kapacitete za digitalnu forenziku. Pored izmena i dopuna krivičnog procesnog zakonodavstva, krivično materijalno pravo treba u stopu da prati razvoj visokotehnološkog kriminala.

Osmo, u kontekstu evrointegracijskog puta BiH, ova država će morati postati deo strateške obaveštajne saradnje o sajber pretnjama i aktivnostima, te uzeti učešće u radu Radne obaveštajne grupe za sajber bezbednost, kada ista bude uspostavljena na nivou EU.

Da zaključimo, usklađenost strateškog i pravnog okvira u Bosni i Hercegovini sa evropskim standardima sajber bezbednosti nalazi se na nivou ukupnih dostignuća ove države na putu ka članstvu u Evropskoj uniji. Da bi se proces usklađivanja ubrzao, potrebno je, pre svega, prevazići unutrašnje podele i neusklađenosti, koje proizilaze iz specifične ustavno-političke koncepcije države, te doneti strateški dokument iz oblasti sajber bezbednosti u što kraćem roku.

8 https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

Literatura

- Bejatović, S. (2012). Visokotehnološki kriminal i krivičnopravni instrumenti suprotstavljanja. *Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal* (pp. 17–30). Laktaši: Visoka škola unutrašnjih poslova.
- Bendiek, A., & Kettemann, M. C. (2021). *Revisiting the EU cybersecurity strategy: a call for EU cyber diplomacy.* (SWP Comment, 16/2021). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2021C16 .
- Blažič, B.J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. *Educ Inf Technol* 27, 3011–3036 (2022). https://doi.org/10.1007/s10639-021-10704-y.
- Bošković, M., Jovičić, D. (2002). *Kriminalistika metodika*. Banja Luka: Viša škola unutrašnjih poslova.
- Brenner S. (2002). *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law&Technology, *4/2002*, pp. 27–29.
- Vranješ, N., Rajčević, S. (2012). Pravni i institucionalni okvir suprotstavljanja visokotehnološkom kriminalitetu u Republici Srpskoj. *Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal* (pp. 119–127). Laktaši: Visoka škola unutrašnjih poslova.
- Directive (EU) 2016/1148 of the European Parliament and of the Council – (EU Network and Information Security Directive) of 6 July 2016 Union.
- Zakon o zaštiti ličnih podataka, Službeni glasnik Bosne i Hercegovine, br. 49/06, 76/11, 89/11.
- Zakon o zaštiti tajnih podataka, Službeni glasnik Bosne i Hercegovine, br. 54/05, 12/09.
- Zakon o informacionoj bezbjednosti, Službeni glasnik Republike Srpske, br. 70/11.
- Zakon o krivičnom postupku Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, br. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13, 65/18.
- Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Službeni glasnik Republike Srbije, br. 10/23.
- Ignjatović, Đ. (1991). *Pojmovno određenje kompjuterskog kriminaliteta*. Anali Pravnog fakulteta u Beogradu, *39(1–3)*, 136–144.
- Konvencija o visokotehnološkom kriminalu, Službeni glasnik BiH – Međunarodni ugovori, br. 06/2006.

- Krivični zakon Bosne i Hercegovine, Službeni glasnik Bosne i Hercegovine, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 8/10, 47/14, 22/15, 40/15, 35/18, 46/21, 31/23, 47/23.
- Krivični zakon Brčko distrikta Bosne i Hercegovine, Službeni glasnik Brčko distrikta Bosne i Hercegovine, br. 19/2020 – prečišćen tekst.
- Krivični zakon Federacije Bosne i Hercegovine, Službene novine Federacije Bosne i Hercegovine, br. 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16, 75/17.
- Krivični zakonik Republike Srpske, Službeni glasnik Republike Srpske, br. 64/17, 104/18, 15/21, 89/21.
- Mijalković, S., Arežina-Đerić, V., Bošković, G. (2010). Korelacija informacione i nacionalne bezbednosti. *Savetovanje o zloupotrebi IT.* Beograd: ZITEH, Dostupno na: https://singipedia.singidunum.ac.rs/izdanje/40146-korelacija-informacione-i-nacionalne-bezbednosti , pristupljeno: 20. 7. 2023.
- Milošević, M., Putnik, N. (2017). *Sajber bezbednost i zaštita od visokotehnološkog kriminala u Republici Srbiji – strateški i pravni okvir*. Kultura polisa, god. *XIV (2017),* br. 33, str. 177–191.
- Novičić, Ž. (2021). Nova strategija sajber bezbednosti EU za digitalnu deceniju — analiza. Razvojni pravci Evropske unije nakon pandemije KOVID 19 / [ed. Nevena Stanković, Dragana Dabić, Goran Bandov]. – ISBN 978-86-7067-289-5. – (2021), str. 123–145.
- Organisation for Economic Co-operation and Development (1986). *Computer – Related Crime: Analysis of Legal Policy.* Paris. Available at: https://unov.tind.io/record/559/ , accessed on: 30. 7. 2023.
- Petrović, L. (2007). *Informaciona sigurnost u savremenom svetu*, Info M – Časopis za informacione tehnologije i multimedijalne sisteme, *broj 24*, Fakultet organizacionih nauka, Beograd, str. 10–11.
- Pravilnik o standardima informacione bezbednosti, broj: 19/6-010-/91-23/12 od 10. 5. 2013. Dostupno na: www.vladars.net/sr-SP-Cyrl/Vlada/Ministarstva/mnk/Documents/Правилник%20о%20мјерама%20информационе%20безбједности_517156617.pdf , pristupljeno: 20. 7. 2023.
- Pruckova, M. (2021). *New EU's cybersecurity package: ambitious proposals, daring tasks and deeper cooperation.* Available at: https://ccdcoe.org/library/publications/new-eus-cybersecurity-package-ambitious-proposals-daring-tasks-and-deeper-cooperation/ , accessed on: 22. 7. 2023.
- Simonović, B. (2004) *Kriminalistika*. Kragujevac: Pravni fakultet.
- *Smjernice za strateški okvir sajber sigurnosti u Bosni i Hercegovini*. (2019). Sarajevo: OEBS. Dostupno na: https://www.osce.org/bs/mission-to-bosnia-and-herzegovina/438386 , pristupljeno: 20. 7. 2023.

- Schreier, F., Weekes, B., Winkler, T. (2010). *Cyber Security: The Road Ahead.* Geneva: DCAF.
- Stephson, P. (2010). *Investigating Computer-Related Crime*, Boca Rato: CRC Press.
- Tasheva, I. (2021). *Cybersecurity post-COVID-19: Lessons learned and policy recommendations*. European View, 20(2), 140–149.
- *The EU's Cybersecurity Strategy for the Digital Decade*, Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint communication to the European Parliament and the Council, Brussels, 16. 12. 2020, JOIN(2020) 18 final.
- United Nations (2005). *Workshop 6: Measures to Combat Computer-related Crime.* Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, 18–25 April 2005 (A/CONF.203/14). Available at: https://www.unodc.org/congress/en/previous/previous-11docs.html , accessed on: 15. 7. 2023.
- Uredba o mjerama informacione bezbjednosti, Službeni glasnik Republike Srpske, br. 91/12.
- Urošević, V., Ivanović, Z., Uljanov, S. (2012). *Mač u World Wide Web-u – Izazovi visokotehnološkog kriminala*. Beograd: „Eternal mix“.
- https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit , accessed on: 20. 7. 2023.
- https://fmpik.gov.ba/bh/aktuelnosti/obavje%C5%A1tenja/308-poziv-za-dostavljanje-primjedbi,-prijedloga-i-komantara-na-zakon-o-informacionoj-sigurnosti-i-sigurnosti-mre%C5%BEnih-i-informacionih-sistema.html, accessed on: 20. 7. 2023.
- Farrand B., Carrapico H. (2022). *Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity*, European Security, 31:3, 435–453, DOI: 10.1080/09662839.2022.2102896.
- Fahey, E. (2022). Developing EU cybercrime and cybersecurity On legal challenges of EU institutionalisation of cyber law-making. In: Hoerber, T., Weber, G. & Cabras, I. (Eds.), *The Routledge Handbook of European Integrations* (pp. 270–284). Abingdon, UK: Routledge. ISBN 9780367203078.
- Šikman, M., Milošević, M. (2012). Normativne pretpostavke za suprotstavljanje visokotehnološkom kriminalitetu u Republici Srbiji i Republici Srpskoj. *Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal* (pp. 3–15). Laktaši: Visoka škola unutrašnjih poslova.

Petar Djukic, MSc
PhD Candidate at the Faculty of Security Studies
University of Belgrade

LEGAL FRAMEWORK FOR PROTECTION AGAINST HIGH-TECH CRIME IN BOSNIA AND HERZEGOVINA – analysis of strategic goals and the possibility of harmonization with the European cyber security strategy

The topic of this paper is the legal framework for protection against high-tech crime in Bosnia and Herzegovina, with an analysis of strategic goals and the possibility of alignment with the EU Cyber Security Strategy for the Digital Decade, which was adopted the year before last. The paper provides a conceptual definition of high-tech crime and cyber security, as well as their basic characteristics. Then, in brief, the legal framework of protection against high-tech crime in Bosnia and Herzegovina was analyzed. When it comes to the EU Cyber Security Strategy for the Digital Decade, the most significant parts of it are interpreted in the continuation of the work, especially those that could have application significance for Bosnia and Herzegovina. Based on the above, appropriate recommendations were given in the final deliberations for the improvement of the legal and strategic framework of cyber security in BiH.

Keywords*: High-tech Crime, Cyber Security, Protection, Strategy, Legal Framework, B&H, European Union.*