PRAVNI ASPEKTI SUPROTSTAVLJANJA SAJBER KRIMINALU U EVROPSKOJ UNIJI

-REVIDIRANI RAD DOI: 10.5937/Oditor2301017B

Iris Bjelica Vlajić[33]

doi: 10.5937/Oditor2302179B

Originalni naučni rad
UDK: 343.53:004.738.5(4-672EU)

Apstrakt

Razvoj informacionih tehnologija i interneta i vršenja krivičnih dela u tom novom okruženju dovodi do pojave transnacionalnog, visokotehnološkog kriminala. Nadležna tela za borbu protiv kriminala u postizanju rezultata sputava tradicionalna podela na nacionalne jurisdikcije dok za izvršioce dela tih ograničenja nema. Sajber aktivnostima nanose se velike štete i posledice fizičkim ili pravnim licima, protivpravno prisvajaju finansijska sredstva i zaštićeni podaci. Specifičnosti visokotehnološkog kriminala zahtevaju specijalizaciju državnih organa jer se u borbi protiv kriminala ne smeju ugroziti individualna prava, privatnost i slobode pojedinaca. Cilj ovog rada je da pokaže kako zakonodavstvo Evropske unije (EU) i aktivnosti njenih institucija unapređuju prevenciju, istragu i krivično gonjenje izvršilaca i grade kapacitete u pravosuđu. Harmonizacija domaćeg prava sa pravom EU u oblasti borbe protiv sajber kriminala predviđena je Poglavljem 24. pregovora „Pravda, sloboda, bezbednost". U odgovaranju na pitanje koji su pravni aspekti suprotstavljanja sajber kriminalu u EU korišćeni su istorijsko-komparativni, metod analize sadržaja i deduktivni metod.

***Ključne reči**: evropsko pravo, sajber kriminal, lični podaci.*

Uvod

Visokotehnološki kriminal, poznat i kao e-kriminal, kibernetički ili sajber kriminal, obuhvata skup krivičnih dela koja podrazumevaju upotrebu interneta, računara ili nekih drugih elektronskih uređaja i pod taj pojam se mogu podvesti različiti oblici krivičnih dela. „U širem smislu, to je kriminalna djelatnost u kojoj su računar ili mreža izvor, sredstvo, predmet, cilj ili prostor krivičnog djela" (Romić et al, 2012). Pojedini oblici e-kriminala direktno su vezani za računare, kao što su širenje opasnih elektronskih virusa ili pokretanje DoS napada (engl. *Denial of Service Attack*) koji onesposobljavaju računarski sistem tako da on odbija da izvrši bilo koju uslugu ovlašćenog korisnika, kada računar postaje

[33] Vanredni profesor dr Iris Bjelica Vlajić, Univerzitet odbrane, Vojna akademija, Veljka Lukića Kurjaka 33, Beograd, R. Srbija, telefon 011/3603171, e-mail: iris_bjelica_vlajic@yahoo.com

predmet napada, dok kod ostalih oblika e-kriminala koji čine prevare, govor mržnje, krivična dela protiv intelektualne svojine, kao i proizvodnja, posedovanje i distribucija spornog materijala, uređaji i internet su sredstvo napada. Kod ove vrste kriminala pored predmeta i sredstva napada, specifično je i mesto izvršenja, a to je paralelni, virtuelni prostor nastao povezivanjem više kompjutera u mreže pogodne za traženje informacija ili za elektronsko poslovanje koji nazivamo sajber prostorom, pri čemu je reč sajber (syber) grčkog porekla i znači nevidljivo, neupadljivo i neograničeno upravljanje. Upravo je ovaj skoro nevidljivi prostor i nepostojanje njegovih ograničenja ono što usložnjava borbu protiv kriminalnih aktivnosti koje se preduzimaju (Bjelajac, Filipović, 2021). Ove specifičnosti utiču na otežano pravno regulisanje materije i problem u procesuiranju izvršilaca, jer sajber kriminal najčešće prevazilazi granice jedne države, odnosno važećeg teritorijalnog zakonodavstva. Izvršiocima ove vrste protivpravnih delatnosti pogoduju slaba zaštita i generalno slaba svest korisnika na mrežama, ali i teškoće otkrivanju izvršenja dela i u prikupljanju dokaza. Iz tog razloga, poslednjih decenija uočljiva je namera najvećeg broja zemalja da kroz različite bilateralne i mutiratelarne sporazume preduzimaju zajedničke akcije kojim bi se udruženo suprotstavile sajber kriminalu. Regulisanje sajber bezbednosti na nacionalnom i međunarodnom nivou doprinosi efikasnijem radu nadležnih tela na otkrivanju izvršenih dela i učinilaca, ali i preventivnom delovanju i sprečavanju vršenja inkriminisanih radnji. Da bi se države adekvatno suprotstavile ovoj pretnji potrebno je njihovo povezivanje i jačenje saradanje i razmene informacija, ali i jačanje saradnje među različitim sektorima unutar države. Pri tome, važno je zaštiti prava pojedinaca na privatnost (Perović, 2018). Tek nakon toga može se pristupati otkrivanju izvršilaca krivičnih dela i izricanju adekvatnih sankcija za odgovorne, bez obzira da li se radi o fizičkim ili pravnim licima.

Prvi dokument kojim se sveobuhvatno nastojao rešiti problem sajber kriminala je Konvenciju o kibernetičkom kriminalu (Convention on Cybercrime, ETS 185), usvojena 23. novembra 2001. godine u Savetu Evrope. Donošenju Konvencije prethodilo je usvajanje većeg broja preporuka kojim su se članice upozoravale na nove pretnje i izazove i zahtevala se njihova zajednička akcija. Konvencija je propisala krivična dela usmerena protiv poverljivosti, integriteta i dostupnosti računarskih podataka i sistema, dajući precizne definicije krivičnih dela, koje omogućavaju vođenje krivičnih postupaka i uklanjaju opasnost od duplog gonjenja u više država. Važan deo Konvencije o visokotehnološkom kriminalu posvećen je obavezama država da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlašćenja, kako bi se omogućilo efikasno otkrivanje i procesuiranje slučajeva kompjuterskog kriminala. Prvi koraci u tom postupku su otkrivanje dela i prikupljanje i obezbeđenje dokaza. Ovim je postavljen okvir za pojedina nacionalna zakonodavstva da preciznije odrede obeležja i karakteristike pojedinih krivičnih dela u vezi računara i sajber prostora, njihove osnovne, lakše ili teže oblike, te da propišu krivične sankcije za njihove učinioce, bez obzira da li

se radi o fizičkim ili pravnim licima. Srbija je potpisala Konvenciju Saveta Evrope o sajber kriminalu. Uz Konvenciju je, u Strazburu 28. januara 2005. godine, usvojen Dopunski protokol o zabrani akata rasističke i ksenofobične prirode učinjenih posredstvom računarskih sistema. Njen značaj se ogleda i u činjenici da su joj pristupile i države koje nisu u Evropi, poput SAD, Kanade, Japana, Dominikanske Republike, Paname, Mauricijusa, Australije, Izraela, Šri Lanke i Južnafričke Republike (Bejatović, 2012).

Pitanje bezbenosti u virtuelnom prostoru delimično regulišu i druge konvencije koje se tiču ove materije, poput: Konvencije o zaštiti prava pojedinca u vezi sa automatskom obradom ličnih podataka, Konvencije o zaštiti dece od seksualne eksploatacije i seksualnog zlostavljanja, te Konvencije o sprečavanju terorizma.

Rad na povezivanju država imala je i Organizacija Ujedinjenih nacija. Različita tela ove organizacije su, u skladu sa svojim ovlašćenjima, delovala u pravcu podizanja svesti i povezivanja članica u suprotstavljanju pretnjama koje visokotehnološki kriminala predstavlja. Rezolucija br. 55/2 Generalne skupštine UN od 18. septembra 2000. godine, poznata i kao Milenijumska deklaracija, među ciljevima za nastupajući milenijum navodi bezbedno i dostupno koišćenje novih tehnologija. Pored toga, Generalna skupština usvojila je niz rezolucija koje se odnose na borbu protiv zloupotrebe informatičkih tehnologija i međunarodnu internet sigurnost.

Zadatak usaglašavanja nacionalnih zakonodavstava u oblasti visokotehnološkog kriminala i bezbednosti u sajber prostoru Ujedinjene nacije dodeljuju Međunarodnoj telekomunikacionoj uniji (ITU), svojoj agenciji za pitanje informacionih i komunikacionih tehnologija (IKT). ITU je maja 2007. godine predstavila dokument pod nazivom Memorandum o globalnoj sajber bezbednosti (A Global Cybersecurity Agenda – GCA) u kom su navedeni osnovni problem i preporuke za poboljšanje bezbednosti.

Takođe, Ekonomsko-socijalni savet Ujedinjenih nacija, u julu 2007. godine, usvojio je Rezoluciju 2007/20, koja govori o međunarodnoj saradnji u oblasti prevencije, istrage, krivičnog progona i kažnjavanja privrednog kriminaliteta i dela povezanih sa zloupotrebom identiteta.

Rešavanju probelema visokotehnološkog kriminala i pretnji po savremeno društvo svojim unutrašnjim dokumentima su se bavile i mnoge druge organizacije, poput NATO, OSCD, OECD, ICANN, AU, ASEAN, OA (Pernik, 2014).

Cilja rada i korišćena metodologija

Cilj rada je davanje odgovora na pitanje koji su pravni aspekti borbe protiv visokotehnološkog kriminala u Evropskoj uniji (EU), jer suprotstavljanje visokotehnološkom kriminalu uključuje različite oblasti, činioce i aspekte. Da bi se odgovorilo na to pitanje, potrebno je bilo definisati osnovne pojmove, prikupiti

podatke puterm istraživanja, klasifikovati ih i analizirati. U tom procesu nametnula su se tri osnovna pitanja:

1. Koji su dokumenti Evropske unije koji uređuju pravne aspekte borbe protiv visokotehnološkog kriminala?
2. Na koji način je to uređeno?
3. U kojoj meri je domaći pravni sistem usklađen sa evropskim?

Naučno istraživanje početni je korak kojim se postojeća znanja verifikuju, a nova stiču, jer deskripcija dosadašnjih aktivnosti predstavlja prvi korak kojim se potpuno, objektivno i sistematično utvrđuje polazno stanje, odnosno utvrđuju se činjenice, dok je analitički metod korišćen za utvrđivanje njihove međusobne uslovljenosti i otkrivanje novih činjenica, njihovih relacija ili posledica. Analiza sadržaja podrazumeva istraživanje i razmatranje velikog broja pravnih izvora, imajući u vidu različita tela Unije i njihova ovlašćenja da donose obavezujuće akte ali i dokumenta koja, mada nisu obavezujuća, imaju značaj za kreiranje politike Unije i njenih članica. Pored akata koja usvajaju njeni organi, Evropska unija potpisuje i pristupa međunarodnim sporazumima koja se donose pod okriljem drugih međunarodnih organizacija, pre svega Organizacije Ujedinjenih nacija i Saveta Evrope. Sva ova pravila formiraju pravni okvir za borbu protiv visokotehnološkog kriminala. U tom smislu, za potrebe pisanja ovog rada analizirani su sledeći tekstovi:

- Komunike o stvaranju bezbednijeg informacionog društva poboljšanjem bezbednosti informacione infrastrukture i borbom protiv kompjuterskog kriminala, (COM (2000) 890 final)
- Okvirna odluka o borbi protiv prevare i fasifikovanja bezgotovinskih sredstava plaćanja, 2001/413/JHA
- Saopštenje o bezbednosti mreže i informacija: Predlog pristupa politici EU (COM (2001)298 final)
- Komunikacija o strategiji za bezbedno informaciono društvo (COM (2006)251 final)
- Komunikacija o borbi protiv neželjene pošte, špijunskog softvera i zlonamernog softvera (COM (2006)688 final)
- Uredba EU/460/2004 o stvaranju Evropske agencije za bezbednost mreža i informacija (ENISA)
- Okvirna odluka EU 2005/222/JHA o napadima na informacione sisteme,
- Direktiva 2002/58/EZ o koja se odnosi na obradu ličnih podataka i zaštitu privatnosti u sektoru elektronskih komunikacija,
- Odluka 2001/413/JHA o borbi protiv prevare i falsifikovanja bezgotovinskih sredstava plaćanja,
- Okvirna odluka EU 2004/68/JHA o seksualnoj eksploataciji dece i dečijoj pornografiji u vezi sa dečjom pornografijom objavljenom korišćenjem informacionih sistema

- Okvirna odluka EU 2008/913/JHA Odluka o borbi protiv rasizma i ksenofobije,
- Direktiva 2006/24/EZ o zadržavanju podataka u vezi sa pružanjem javnih elektronskih komunikacionih usluga,
- Okvirna odluka 2005/222/JHA o napadima na informacione sisteme,
- Evropska bezbednosna strategija "Evropska unutrašnja strategija bezbednosti u akciji: pet koraka ka bezbednijoj Evropi",
- Direktiva 2013/40/EU o napadima na informacione sisteme,
- Evropska bezbednosna strategija „Bezbednij Evropa u boljem svetu"
- Predlog Uredbe za obezbeđivanje pristupa i čuvanja dokaza COM(2018) 225 final- 2018/0108(COD) i
- Predlog Direktive o imenovanju pravnih zastupnika COM/2018/226 final - 2018/0107 (COD),
- Direktiva EU/019/713 o o borbi protiv prevare i fasifikovanja bezgotovinskih sredstava plaćanja
- Uredba EU/2019/881 o ENISA (Evropskoj Agenciji za sajber bezebdnost**)** i o informacionim i komunikacionim tehnologijama sertifikacije sajber bezbednosti i izmeni Uredbe EU/526/2013.

Nakon utvrđivanja polaznih osnova, pristupljeno je klasifikaciji podataka prema prirodi ili svojstvima. Sinteza prikupljenih znanja i iznošenje rezultata istraživanja dati su u fomi zaključka da Unija, u skladu sa svojim ovlašćenjima, radi na stvaranju koherentnog pravnog okvira koji obavezuje na delovanje različite aktere.

Rezultati rada sa diskusijom

Razvoj informacionog društva i novih tehnologija doprineli su konkurentnosti, privrednom rastu i lakšem zapošljavanju unutar Unije, ali su i izložili pravna i fizička lica riziku od sajber napada. I, dok su Savet Evrope i Ujedinjene nacije ubrzano radili na definisanju visokotehnološkog kriminala i izradi metodologije za borbu protiv njega, Evropska unija je nije pokazivala nikakvo interesovanje za ovu oblast, kao da je čekala da vidi ishod aktivnosti koje su se dešavale pod okriljem pomenute dve organizacije. Tek, naknadno, ona počinje da usvaja legislativu koja za temu ima borbu protiv visokotehnološkog kriminala. Vremenom, rad EU na uređenju okvira za bezbedno korišćenje računara i virtuelnog prostora postaje sve značajniji jer je siguran internet prostor od ključnog značaja za funkcionisanje i razvoj unutrašnjeg tržišta (De Hert et al, 2006). Osnov za to nalazi se u članu 16. Ugovora o formiranju EU (UFEU), poznatom još kao Lisabonski ugovor, koji uvodi poseban pravni osnov za donošenje pravila koja se odnose na zaštitu pojedinaca u pogledu obrade ličnih podataka od strane institucija Unije, od strane država članica kada obavljaju aktivnosti koje spadaju u delokrug prava Unije, i pravila koja se odnose na slobodno kretanje takvih podataka. Pošto Unija ima pre svega političko-

ekonomski karakter, njene osnovne oblasti delovanja su saradnja policijskih i pravosudnih tela u toj borbi i razvoj međunarodne saradnje, ali i usvajanje domaćih pravnih normi u državama članicama koje će stvoriti adekvatne i efikasne pravne instrumente za suprotstavljanje sajber kriminalu, koje će biti primenjive, racionalne, efikasne i pravične (Bejatović, 2012).

Prvi dokument usvojen 2001. godine pod nazivom „Komunike o stvaranju bezbednijeg informacionog društva poboljšanjem bezbednosti informacione infrastrukture i borbom protiv kompjuterskog kriminala“ predlaže saradnju u mnogim oblastima, a posebno izmenu zakonodavstva kojim bi se obuhvatila dela visokotehnološkog kriminala i usaglasila kaznena politika članica u pogledu tih dela, kao i međusobno priznanje izrečenih presuda. Ovo je bio važan, prvi korak, jer do tada mnogim zemljama krivična dela vezana za visokotehnološki kriminal nisu postojala. Naveden je i značaj saradnje svih zainteresovanih u prikupljanju i očuvanju dokaza jer to nije pitanje koje se isključivo tiče pravosudnih organa, već i privrede i pojedinaca. Ovako postavljen komunike doveo je do pokretanja niza aktivnosti i usvajanja novih dokumenata, među kojim je prvi bila Okvirna odluka o borbi protiv prevare i fasifikovanja bezgotovinskih sredstava plaćanja kojom su se zaštitila sva plaćanja unutar Unije.

Agencija EU za saradnju pravosudnih institucija država članica u krivičnim stvarima (EUROJUST) osnovana je radi borbe protiv prekograničnog kriminala i organizovanih kriminalnih grupa. U sklopu mandat EUROJUST osnovana je jedinica za saradnju između tužilaštava za borbu protiv različitih oblika kriminala među kojim je bio i sajber kriminal. Postignut je dogovor o izdavanju Evropskog naloga za hapšenje (EAW). Mehanizam izdavanja i reagovanja po evropskom nalogu za hapšenje jedan je od od najznačajnih instrumenata koji evropsku pravosudnu saradnju ubrzava i pospešuje. Među krivičnim delima za koja je moguće izdati EAW, navedeni su sajber kriminal, prevare tokom bezgotovinskog plaćanja i falsifikovanje (Wennerström, 2010).

Saopštenje o bezbednosti mreže i informacija (COM (2001)298 final) prvi je formulisani predlog za politiku EU. Politika sajber bezbednosti je od tada razvijena kroz niz akcija, kojima se predstavlja strategiji za bezbedno informaciono društvo, bori protiv neželjene pošte, špijunskog softvera i zlonamernog softvera i koji dovode do stvaranja Evropske agencije za sigurnost na mreži (ENISA) 2004. godine. Pored konkretnih rešenja koja su ponuđena za uočene probleme, značaj ovih aktivnosti je bio u podizanju svesti o značaju problema sigurnosti na internetu, saradnji i odgovornijem korišćenju informacionih tehnologija. Komunikacije su bile osnov za usvajanje novih dokumenata kojima se nastalo predupreditи izvršenje dela ili sprečiti nastajanje značajnih posledica.

Okvirna odluka EU 2005/222/JHA o napadima na informacione sisteme od 24. februara 2005. godine kao osnovni cilj postavlja unapređenje saradnje između

pravosudnih i drugih nadležnih organa, uključujući policiju i druge specijalizovane službe za provođenje zakona, kroz približavanje nacionalnih pravila krivičnog prava u oblasti napada na informacione sisteme. Odluka je predvidela rok od dve godine za svoju implementaciju, ističući time hitnost u postupanju nadležnih organa članica da bi unapredile saradnju i počele da razmenjuju sve relevantne informacije i uspostavljaju operativne kontaktne tačke koje rade bez prestanka. Predstavlja pokušaj prevazilaženja značajnih praznina i razlika u nacionalnim zakonima, koje su otežavale policijsku i pravosudnu saradnju u borbi protiv organizovanog kriminala i terorizma. Odluka sledi pristup koji ima Konvencija Saveta Evrope, i zahteva od država članica EU da kriminalizuju namerni, nezakonit pristup informacionim sistemima, nezakonito mešanje u sistem i nezakonito preuzimanje podataka. Takva dela moraju biti kažnjena delotvornim, srazmernim i odvraćajućim krivičnim kaznama, a krivično delo u kontekstu kriminalne organizacije, koje prouzrokuje značajan gubitak ili utiče na bitne interese, se mora smatrati otežavajućom okolnosti.

EU se prvi put pozabavila neželjenom e-poštom u svojoj Direktivi 2002/58/EZ o privatnosti i elektronskim komunikacijama koja se odnosi na obradu ličnih podataka i zaštitu privatnosti u sektoru elektronskih komunikacija, navodeći da jedinstveno tržište zahteva usklađen pristup u ovoj oblasti jer obim neželjene pošte može izazvati poteškoće za elektronske komunikacione mreže i opremu. Pri tome nije relevantno da li se pretplatnicima veb-sajtova ili elektronskih oglasnih tabli narušavanje privatnosti neželjenom komunikacijom u svrhe direktnog marketinga, vrši putem sredstava automatizovanih mašina za pozivanje, faksova i e-pošte, ili SMS poruka. Paralelno sa zaštitom podataka i borbom protiv prevare i falsifikovanja bezgotovinskih sredstava plaćanja, Evropska unija se bori protiv seksualne eksploatacije dece i dečije pornografije objavljene korišćenjem informacionih sistema i protiv bilo kog oblika rasizma i ksenofobije.

Usledilo je usvajanje nekoliko preporuka članicama u različitim formama, od kojih je najznačajnija bila Direktiva 2006/24/EZ o zadržavanju podataka u vezi sa pružanjem javnih elektronskih komunikacionih usluga i izmeni Direktive 2002/58/EZ, što je bio važan korak ka uspostavljanju harmonizovanog sistema za prikupljanje i skladištenje podatke o saobraćaju u EU, i Okvirna odluka 2005/222/JHA o napadima na informacione sisteme. Direktiva je usvojena na osnovu zaključaka Saveta za pravosuđe i unutrašnje poslove od 19. decembra 2002. godine, u kojima je posebno istaknuto da, zbog značajnog rasta mogućnosti koje pružaju elektronske komunikacije, podaci koji se odnose na korišćenje elektronskih komunikacija su dragoceno sredstvo u prevenciji, istrazi, otkrivanju i krivičnom gonjenju krivičnih dela, posebno organizovanog kriminala. Okvirna odluka, s druge strane, bila je pokušaj Evropske unije da postigne minimalni nivo približavanja u pogledu tri kompjuterska krivična dela (nezakonit pristup informacionim sistemima, nezakonito ometanje sistema, nezakonito ometanje podataka), čije se definicije u velikoj meri zasnivaju na onim iz Konvencije

Saveta Evrope o sajber kriminalu. Međutim, iznenađujuće je da Okvirna odluka nije dostigla viši nivo približavanja nego što je postigla Konvencija Saveta Evrope u pogledu primenljivih sankcija. Član 6. Okvirne odluke predviđa niz „minimalnih-maksimalnih" sankcija, koje za nezakonito ometanje sistema i nezakonito ometanje podataka moraju biti između 1 i 3 godine zatvora. Od država članica je zatraženo da implementiraju ove odredbe do kraja 2007. godine. Uprkos različitim dokumentima i pokušajima stvaranja koherentnog sistema koji bi olakšao članicama povezivanje, saradnju i usglašavanje aktivnosti u zaštiti pojedinaca, kompanija i institutcija od sajber napada, značajniji rezultati su izostali zbog strukture i organizacije Evropske zajednice. Usvajanjem Ugovora o funkcionisanju Evropke unije (Lisabonski ugovor - UFEU), Uniji su data nova ovlašćenja i mogućnosti za delovanje na polju unutrašnje bezbednosti. Odmah po stupanju na snagu Lisabonskog ugovora usvojeni su Stokholmski program 2009. godine i Strategija unutrašnje bezbednosti početkom 2010. godine (Nikodinovska-Stefanovska, Đurovski, 2012). Krajem 2010. godine, Evropska komisija je u saradnji sa Evropskim parlamentom i Savetom Evropske unije izradila dokument pod nazivom "Evropska unutrašnja strategija bezbednosti u akciji: pet koraka ka bezbednijoj Evropi", navodeći da sistem bezbednosti sajber prostora ima pet strateških prioriteta: postizanje elastičnosti, u smislu da se sistemi automatski vraćaju u normalno stanje nakon incidenta, značajno smanjenje sajber kriminala, razvoj politike sajber odbrane i kapaciteta saglasnih Zajedničkoj bezbednosnoj i odbrambenoj politici (Common Security and Defence Policy - CSDP), razvoj industrijskih i tehnoloških resursa za sajber bezbednost i uspostavljanje povezanih međunarodnih politika sajber bezbednosti za Uniju i promovisanje osnovnih vrednosti Evropske unije.

Najambiciozniji instrument EU usvojen u tom periodu je Direktiva o napadima na informacione sisteme (2013/40/EU) od 12. avgusta 2013. godine kojom se potencira bezbednosti mreža i informacija (NIS) i uvodi obaveza izveštavanja o incidentima za privatni sektor (uključujući operatere osnovnih usluga i digitalnih usluga). Direktiva propisuje mere za osiguranje visokog zajedničkog nivoa mrežne i informacione bezbednosti širom Unije, kojim se od zemalja članica zahteva izrada nacionalne strategije za mrežnu i informacionu bezbednost (NIS), kao i kooperacioni plan kojima se omogućava sprovođenje NIS. Članice su u obavezi da formiraju stručne nacionalne timove, pre svega tim nadležan za kompjuterske incidente (Computer Emergency Response Team – CERT) koji po uspostavljanju sarađuju sa policijskim agencijama na prevenciji, otkrivanju i odgovoru na sajber napade, ali i zadatkom da razviju nacionalne planove za nepredviđene situacije. Za institucije EU, 2012. godine, uspostavljen je CERT-EU. Razvija se Evropski sistem za razmenu informacija i upozorenja (European information sharing and alert system - EISAS) kao mreža kontakata među članicama i drugim relevantnim telima. U državama članicama formiraju se Nacionalni kompetentni autoriteti, kao najznačajnije domaće institucije sa

zadatkom da prate primenu Direktive na nacionalnom nivou i sarađuju sa istim telima drugih država članica, bezbednosnim službama i telima za zaštitu podataka, kao i da postupaju po primljenim obaveštenjima o incidentima koje im upute javna administracija i javni operateri telekomunikacionih i informacionih usluga. Pored osnovna dva tela, svaka država članica može da formira: telo za informacionu bezbednost (IAA), telo za TEMPEST (TA), telo za odobravanje kriptografskih rešenja (CAA) i telo za distribuciju kriptografskih materijala (CDA).

Strategija nacionalne bezbednosti predstavlja opšte programsko stanovište jedne države u oblasti njene bezbednosti (Nedeljković, Forca, 2018). EU je usvojila Evropsku strategiju bezbednosti „Bezbednija Evropa u boljem svetu“ (A safer Europe in a better world, European security strategy) 2013. godine sa ciljem jačanja sajber bezbednosti javne administracije i kritične infrastrukture u kojoj ističe potrebu za razvitkom strateške kulture radi rane i brze intervencije u situacijama kada je bezbednost na bilo koji način ugrožena. Strategija ima tri poglavlja: analizu bezbednosnog okruženja, u kojem su predstavljeni globalni izazovi i ključne pretnje; definisanje strateških ciljeva i procena političkih implikacija za Evropu i usmerena na borbu protiv visokotehnološkog kriminala kroz fokusiranje na partnerstvo sa privredom i izgradnju kapaciteta unutar država članica za suprotstavljanje sajber napadima (Carrapico, Barinha, 2018). U okviru postojećih struktura EUROPOL, Unija je 2013. godine, osnovala Kriminalistički centar za visoke tehnologije (E/C3), putem kog države članice i institutcije Unije izgrađuju i unapređuju operativne i analitičke kapaciteta za sprovođenje istraga i saradnju sa međunarodnim partnerima. Centar sarađuje sa Evropskom agencijom za bezbednost mreža i informacija (European Network and Information Security Agency - ENISA) kao i mrežom nacionalnih timova za računarske incidente (CERTs). Evropska agencija za mrežnu i informacionu bezbednost (ENISA) formirana je 2004. godine Uredbom Evropske komisije i Saveta broj EZ/460/2004 sa ograničenim mandatom koji se od tog dana produžavao. U aprilu 2019. godine doneta je nova Uredba kojom je ENISA preimenovana u Evropsku agenciju za sajber bezbednost i data su joj nova ovlašćenja i dodata nova tela. Sedište Agencije je u Atini, ima status pravnog lica, a finansira se od sredstava iz budžeta Evropske unije, sredstava trećih zemalja koje učestvuju u radu Agencije, kao i donacija država članica u novcu ili naturi. Prvobitni zadatak ENISA da vrši poslove radi uspostavljanja visokog nivoa bezbednosti mreža i podataka u Evropskoj uniji, podizanja svesti o informacionoj bezbednosti i razvoja i promovisanja kulture bezbednosti mreža i podataka za dobrobit građana, potrošača, preduzeća i organa javne vlasti Evropske unije proširen je pogledu sertifikacije sajber bezbednosti. U svakoj od država članica ENISA ima najširu poslovnu sposobnost koja pravna lica imaju po unutrašnjem pravu članice i može da zaključuje ugovore u skladu sa pravom koje se primenjuje na konkretan ugovorni odnos. Ovlašćena je da sarađuje sa trećim zemljama i međunarodnim

organizacijama radi promovisanja međunarodne saradnje u oblasti bezbednosti mreža i podataka. Organi ENISA su: Upravni odbor, Izvršni odbor, izvršni direktor, Stalno telo zainteresovanih strana (koje uključuje predstavnike akademske zajednice, privrede i potrošača) i ad hoc radne grupe. Od 2019. godine postoji i stalno telo koje čine nacionalni oficiri za vezu, a ENISA je odgovrna za šemu sertifikacije za sajber bezbednost za proizvode, usluge i procese za podršku jedinstvenom digitalnom tržištu.. Evropski parlament, Savet, Evropska komisija i nadležna regulatorna tela država članica mogu da podnose zahteve za savete i podršku.

Savet Evropske unije, u junu 2017. godine, odobrio je Set alata za sajber diplomatiju sa krajnjim ciljem da ojača aktivnosti EU i potencira koordinisan odgovor u slučaju sajber napada protiv evropskih ciljeva. Najvažniji akteri u ovoj oblasti, u skladu sa tim setom su: Evropska agencija za bezbednost mreža i informacija (ENISA), Evropska policijska kancelarija (EUROPOL) uključujući Evropski centar za sajber kriminal (E/C3) i Evropska odbrambena agencija (EDA). Evropska komisija, izvršno telo EU, uključena je u formulisanje politike sajber bezbednosti Unije, prioriteta i ciljeva preko Generalnog direktorata za unutrašnje poslove (DG Home) koji je odgovoran za saradnju policije i krivičnog pravosuđa i nadgleda aktivnosti Evropola, dok je njegov deo DG Connect zadužen za zaštitu kritične infrastrukture i nadgleda aktivnosti ENISA. EDA je zadužena za dalji razvoj sajber sposobnosti EU zajedno sa Vojnim štabom EU (EUMS). Jedinica za pravosudnu saradnju (EUROJUST) ima ulogu u borbi protiv sajber-kriminala olakšavajući saradnju među tužiocima. Dvogodišnji projekat COURAGE (Cibercrime and Ciberterrorism European Research Agenda) iz Sedmog okvirnog programa EU isporučio je sveobuhvatnu agendu istraživanja i usklađenu mapu puta na osnovu saradnje sa 17 organizacija iz 12 evropskih zemalja na terenu. Konačni rezultati projekta objavljeni u maju 2016. godine identifikovali su nedostajuća rešenja za bolju primenu postojećih pravila i preporučili njihovu korekciju (Jerman-Blažič et al, 2016).

Zbog potrebe pvezivanja Unije sa drugim akterima u borbi protiv visokotehnološkog kriminala Evropska komisija je 2018. godine predstavila osnove za dva seta pregovora, sa Sjedinjenim Državama (SAD) i za Drugi dodatni protokol uz „Budimpeštansku“ konvenciju Saveta Evrope o sajber kriminalu. Oba dokumenta predviđaju snažne mere zaštite podataka i privatnosti, a tiču se obezbeđenja prekograničnog pristupa elektronskim dokazima u krivičnim istragama. U pregovorima sa SAD predlaže se uvođenje obavezujućeg evropskog naloga za dostavljanje i evropskog naloga za čuvanje dokaza. Oba naloga mora izdati ili overiti pravosudno telo države članice. Može se izdati nalog kojim se traži čuvanje ili dostavljanje podataka koje pohranjuje pružalac usluga koji se nalazi u drugoj državi, a koji su potrebni kao dokaz u kriminalnim istragama ili postupcima. Drugim aktom, uvodi se obaveza da pružaoci usluga imenuju pravnog zastupnika u Uniji koji će osigurati prijem, poštovanje i izvršavanje

odluka kako bi nadležna nacionalna tela mogla prikupiti dokaze u krivičnim postupcima. Smanjenjem prepreka koje proizlazi iz toga osiguralo bi se bolje funkcioniranje unutrašnjeg tržišta na način koji je dosledan s razvojem zajedničkog područja slobode, sigurnosti i pravde.

Značajan iskorak u borbi protiv sajber kriminala je Direktiva 2019/713/EU o prevarama pri bezgotovinskom plaćanju, kojom se ažurira pravni okvir, uklanjaju prepreke za operativnu saradnju i povećava prevencija i pomoć žrtvama, kako bi radnje za sprovođenje zakona protiv prevara i falsifikovanja bezgotovinskih sredstava plaćanja bile efikasnije. Poslednji u nizu akata koji su vezani za sigurnost na internetu je Privremeni propis za regulisanje obrade ličnih i drugih podataka sa ciljem borbe protiv seksualne zloupotrebe dece od 10. septembra 2020. godine nastao na osnovu Direktive 2002/58/EZ.

Republika Srbija usvojila je Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (VTK Zakon) 2005. godine, kojim je uspostavljen institucionalni okvir za borbu protiv sajber kriminala jer je Zakon predvideo formiranje specijalizovane jedinice MUP, kao i posebnih sudskih i tužilačkih tela za borbu protiv visokotehnološkog kriminala, Posebno tužilaštvo za visokotehnološki kriminal kao deo Višeg javnog tužilaštva u Beogradu, Viši sud kao prvostepeni sud, i Apelacioni sud u Beogradu kao drugostepeni sudski organ. Zakon je donet posle usvajanja Budimpeštanske konvencije i Dodatnog protokola bio je usklađen sa njima, čime je počela primena međunarodnih standarda važnih za ovu oblast. Krivičnim zakonik Republike Srbije usvojen 2005 godine, u pravni sistem uvodi kompjuterska krivična dela. Narodna skupština Republike Srbije početkom 2009. godine posebnim zakonima ratifikovala Budipeštansku konvenciju i Dodatni protokol, ali i usvojila nove i dopunila postojeće zakonske i podzakonske akte od značaja. U skrining izveštaju za Poglavlje 24 „Pravda, sloboda, bezbednost“ koji je urađen 2014. godine nalaz Evropske komisije je bio da se Srbija nalazi među zemljama u kojim je rizik od sajber napada veći zbog čega je neophodno nastaviti rad na osposobljavanju nadležnih tela za porbu protiv tih napada, ali i na podizanju svesti korisnika o rizicima kojim su izloženi (Krivokapić, Petrovski, 2016).

Zakonom o elektronskim komunikacijama prvi put su uređuni uslovi i način za obavljanje delatnosti u oblasti elektronskih komunikacija, nadležnosti državnih organa, kao i zaštitu prava korisnika i pretplatnika, bezbednost i integritet elektronskih komunikacionih mreža i usluga, tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka, kao i druga pitanja od značaja za funkcionisanje i razvoj elektronskih komunikacija u Republici Srbiji. Zakon je usvojen sa namerom da se zaštiti privatnost korisnika od nedozvoljenog pristupa njihovim digitalnim zapisima i podacima sa njihovih profila (Darijević, 2021).

Pored zakonskih i podzakonskuih akata, usvojena je Strategija razvoja informacionog društva 2010 - 2020. godine i urađena procena pretnje od teškog i

organizovanog kriminala u Srbiji (Serious and Organised Crime Threat Assessment - SOCTA) 2015. godine. Procena je strateški dokument koji razmatra različite oblike teškog i organizovanog kriminala, uključujući i sajber kriminal, koji daje osnovu za operativni rad policija u skladu sa postojećim trendovima (Krivokapić, Petrovski, 2016).

Zakon o informacionoj bezbednosti koji je stupio na snagu u februaru 2016. godine, odnosi se na pravna lica. Propisano je osnivanje institucija među kojima je najznačajniji Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima, domaći CERT tim. Njemu je dato u nadležnost prikupljanje informacija, klasifikacija informacija o incidentima i rizicima, podizanje svesti kod građana i saradnja sa javnim i privrednim subjektima (Đukić, 2018). Nakon toga, u martu 2016. godine, osnovano je Telo za koordinaciju poslova informacione bezbednosti, čime se Republika Srbija uključila u mrežu nacionalnih tela za razmenu informacija i borbu protiv kriminala kako je to propisano Direktivom 2013/40/EU.

Zaključak

Informaciona bezbednost je definisana kao skup mera koje omogućavaju da podaci kojima se rukuje putem kompjuterskih sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica. Pošto EU, za razliku od nekih drugih organizacija, nema kapacitet da pruži direktnu pomoć članicama koje su pod sajber napadom, ona deluje kao posrednik koji pomaže u razmeni znanja i iskustva i podržava usvajanje najbolje prakse za pojedinačne probleme. Uloga koju EU ima u pogledu obuke, saradnje i povezivanja članica u borbi protiv visokotehnološkog kriminala, kao i privatno-javno partnerstvo koje se pokazuje neizostavnim u uspešnom otkrivanju, prikupljanju i čuvanju dokaza, koje je u Uniji osnovni način delovanja povećava značaj EU u borbi protiv sajber kriminala. Oslanjanjući se na ovlašćenja koja je dobila Lisabonskim ugovorom (UFEU) Unija sistematično stvara jedinstven pravni okvir kojim se u potpunosti identifikuju odgovorni za suprotstavljanje sajber napadima, usaglašava i dopunjuje materijalno i procesno krivično pravo članica, i tako pojačava sistem unutrašnje bezbednosti Unije kao celine.

Srbija je potpisala Konvenciju Saveta Evrope o sajber kriminalu i u velikoj meri je uskladila svoje zakonodavstvo sa Direktivom o napadima na informacione sisteme iz 2013. godine. Potrebne su izmene i dopune zakona, posebno u delu koji se odnosi na obezbeđenje i prikupljanje dokaza i na sankcije, kako bi u potpunosti zakonodavstvo bilo usklađeno sa regulativom EU. U Izveštaju o napretku Srbije u 2014 i 2015, Komisija EU je istakla da je neophodno da se dodatno uskladi pravni okvir koji se odnosi na dečju pornografiju. Jedan od zahteva je bilo i usvajanje

strategije o visokotehnološkom kriminalu. Vlada Srbije je Akcionim planom za Poglavlje 24 obezbedila mere kojim će uskladiti svoje zakone sa zakonodavstvom i standardima Evropske unije za borbu protiv visokotehnološkog kriminala kroz analizu postojećeg zakonskog okvira, izradu nacrta zakona i drugih propisa na osnovu analize u cilju poboljšanja organizacionih, ljudskih i tehničkih kapaciteta organa zaduženih za borbu protiv visokotehnološkog kriminala, a pre svega obuka zaposlenih u Posebnom javnom tužilaštvu i policijskoj jedinici za visokotehnološki kriminal. Akcionim planom za Poglavlje 24 predviđena je i dodatna specijalizovana obuka u cilju jačanja kapaciteta državnih organa odgovornih za borbu protiv visokotehnološkog kriminala. Unutar Odeljenja za visokotehnološki kriminal MUP uspostavljene su specijalizovane jedinice za istrage zloupotreba kreditnih kartica, internet trgovine i internet bankarstva i jedinica za suzbijanje ilegalnog i štetnog sadržaja na internetu što bi trebalo doprineti kvalitetnijem vođenju istraga i prikupljanju dokaza. Navedenim izmenama zakonodavstva i osnivanjem nacionalnih tela, Srbija je ispunila minimum uslova predviđen pravnim okvirom Unije za suprotstavljanje sajber napadima.

Pored stručnih tela koja se bave otkrivanjem i gonjenjem učinilaca krivičnih dela, neophodna je saradnja između privatnog i javnog sektora, organizacija civilnog društva koja se bave visokotehnološkom bezbednosti i borbom protiv visokotehnološkog kriminala i akademske zajednice. Mnoge države su izuzetno spore i neadekvatno obučene za odgovor na ove pretnje, što se može popraviti boljom međunarodnom razmenom iskustava i dosadašnje prakse u polju bezbednosti u sajber prostoru, a što je olakšano usvajanjem velikog broja multilateralnih sporazuma.

Literatura

1. Bejatović S., 2012. Visokotehnološki kriminal i krivičnopravni instrumenti suprotstavljanja, Zbornik radova Međunarodna naučnostručna konferencija „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal“, Visoka škola unutrašnjih poslova Republike Srpske: 17- 30 (dostupno na: http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)
2. Bjelajac Ž., A.Filipović. 2021. Specific characteristics of digital violence and digital crime, Law theory and practice (4): 16 – 32
3. Carrapico H., A. Barinha.2018. European Union cyber security as an emerging research and policy field, Symposium: European Union cyber security as an emerging research and policy field, European Politics and Society, 19 (3): 299-303
4. Csonka P. 2006. The Council of Europe's Convention on cyber-crime and other European initiatives, Revue international de droit penal, 3-4 (77): 473 - 501

5. Darijević V. 2021. Sajber kriminal kao bezbednosni rizik na internetu, Megatrend revija, 2(18): 257-266
6. De Hert, P., G. González Fuster, B-J. Koops. 2006. Fighting cybercrime in the two Europes, The added value of the EU framework decision and the council of Europe Convention, Revue internationale de droit pénal 3-4 (77): 503-524
7. Đukić A. 2018. Organizovani visokotehnološki kriminal – pojam, razvoj i osnovne karakteristike, Vojno delo (3):128-156
8. Jerman-Blažić, B., T. Klobučar, J. Stefan.2016.Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda, European Intelligence and Security Informatics Conference (dostupno na web sajtu: https://web.archive.org/web/20190223201002id_/http://pdfs.semanticscholar.org/4ca3/37b1bc74362b632095de1c40cf7c835498b7.pdf)
9. Krivokapić, D. i A. Petrovski.2016. Sajber kriminal u Srbiji pred otvaranje poglavlja 24 (Pravda, sloboda i bezbednost), Share fondacija (dostupno na web sajtu: https://bezbednost.org/wp-content/uploads/2020/06/sajber_kriminal_u_srbiji_pred_otvaranje_poglavlja_.pdf)
10. Nedeljković, S. i B. Forca. 2015. Evropska strategija bezbednosti i sajber pretnje – značaj za Srbiju, Vojno delo 3: 135-155
11. Nikodinovska-Stefanovska, S. i M. Đurovski.2012. Unutrašnja bezbednost EU i policijska saradnja u postlisabonskoj eri, u Zborniku radova Međunarodna naučnostručna konferencija „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal“, Visoka škola unutrašnjih poslova Republike Srpske: 385 – 395 (dostupno na: http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)
12. Pernik, P. 2014. Improving Cyber Security: NATO and the EU International Centre for Defence Studies (dostupno na web sajtu: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf)
13. Perović, M. 2018. Sajber kriminal kao globalna prijetnja u svijetu, Vojno delo 3: 157-164
14. Romić, M. i N. Grbić-Pavlović. 2012. Međunarodnopravni dokumenti kojima se uređuje oblast visokotehnološkog kriminla u zborniku radova Međunarodna naučnostručna konferencija „Suzbijanje kriminala i evropske integracije, s osvrtom na visokotehnološki kriminal“, Visoka škola unutrašnjih poslova Republike Srpske: 193-217 (dostupno na: http://education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)
15. Wennerström E. 2010. EU-legislation and Cybercrime: A Decade of European Legal Developments, Stockholm Institute for Scandianvian Law,

47-21: 452-472 (dostupno na web sajtu: https://scandinavianlaw.se/pdf/47-21.pdf)

Datum prijema (Date received): 12.09.2022.
Datum prihvatanja (Date accepted): 23.12.2022.

LEGAL ASPECTS OF FIGHTING CYBER CRIME IN THE EUROPEAN UNION

- REVISED PAPER DOI: 10.5937/Oditor2301017B

Iris Bjelica Vlajić [34]

Original scientific paper

Abstract

The development of information technologies and the Internet and the commission of criminal acts in this new environment leads to the emergence of transnational, high-tech crime. Competent bodies for the fight against crime are hindered in achieving results by the traditional division into national jurisdictions, while there are no such restrictions for perpetrators. Cyber activities cause great damage and consequences to natural or legal persons, illegally appropriate financial resources and protected data. The specificities of high-tech crime require the specialization of state authorities because in the fight against crime, individual rights, privacy and freedoms of individuals must not be jeopardized. The aim of this paper is to show how the legislation of the European Union (EU) and the activities of its institutions improve the prevention, investigation and prosecution of perpetrators and build capacities in the judiciary. Harmonization of domestic law with EU law in the field of combating cybercrime is provided for in Chapter 24 of the "Justice, Freedom, Security" negotiations. In answering the question of what are the legal aspects of combating cybercrime in the EU, historical-comparative, content analysis and deductive methods were used.

Keywords: *European law, cybercrime, personal data.*

Introduction

High-tech crime, also known as e-crime, cybernetic or cybercrime, includes a set of criminal acts that involve the use of the Internet, computers or some other electronic devices, and various forms of criminal acts can be subsumed under this term. "In a broader sense, it is a criminal activity in which a computer or a network is the source, means, object, goal or space of a criminal act" (Romi ć et al, 2012). Certain forms of e-crime are directly related to computers, such as the spread of dangerous electronic viruses or the launch of DoS attacks (*Denial of Service Attacks)* that disable the computer system so that it refuses to perform any

[34] Associate Professor Iris Bjelica Vlajić, Ph.D., University of Defense, Military Academy, Veljka Lukića Kurjaka 33, Belgrade, R. Serbia, telephone 011/3603171, e-mail: iris_bjelica_vlajic@yahoo.com

service of the authorized user, when the computer becomes the object attacks, while in other forms of e-crime that include fraud, hate speech, crimes against intellectual property, as well as the production, possession and distribution of disputed material, devices and the Internet are a means of attack. In this type of crime, in addition to the object and the means of attack, the place of execution is also specific, which is a parallel, virtual space created by connecting several computers in networks suitable for searching for information or for electronic business, which we call cyber space, where the word is cyber (syber). of Greek origin and means invisible, inconspicuous and unlimited management. It is this almost invisible space and the absence of its limitations that complicates the fight against criminal activities that are undertaken (Bjelajac, Filipović, 2021). These specificities affect the difficult legal regulation of the matter and the problem in prosecuting the perpetrators, because cybercrime most often exceeds the borders of one country, that is, the valid territorial legislation. Perpetrators of this type of illegal activities benefit from weak protection and generally low awareness of users on the networks, but also difficulties in detecting the commission of the act and in gathering evidence. For this reason, in recent decades, the intention of the largest number of countries to undertake joint actions through various bilateral and multilateral agreements to jointly oppose cybercrime is noticeable. The regulation of cyber security at the national and international level contributes to the more efficient work of competent bodies in the detection of committed acts and perpetrators, but also to preventive action and prevention of incriminated acts. In order for states to adequately oppose this threat, it is necessary to connect them and strengthen cooperation and exchange of information, but also to strengthen cooperation between different sectors within the state. In doing so, it is important to protect the rights of individuals to privacy (Perović, 2018). Only after that can one approach the discovery of perpetrators of criminal acts and the imposition of adequate sanctions for those responsible, regardless of whether they are natural or legal persons.

The first document that comprehensively attempted to solve the problem of cybercrime was the Convention on Cybercrime (ETS 185), adopted on November 23, 2001 by the Council of Europe. The adoption of the Convention was preceded by the adoption of a number of recommendations warning the members of new threats and challenges and demanding their joint action. The Convention has prescribed criminal offenses directed against the confidentiality, integrity and availability of computer data and systems, providing precise definitions of criminal offences, which enable the conduct of criminal proceedings and eliminate the danger of double prosecution in several countries. An important part of the Convention on high-tech crime is devoted to the obligations of states to create normative assumptions for the introduction of additional procedures and powers, in order to enable effective detection and processing of computer crime cases. The first steps in that procedure are the discovery of the crime and the collection and

securing of evidence. This sets the framework for individual national legislations to more precisely determine the features and characteristics of individual criminal acts related to computers and cyberspace, their basic, lighter or more serious forms, and to prescribe criminal sanctions for their perpetrators, regardless of whether they are physical or legal entities. Serbia has signed the Council of Europe Convention on Cybercrime. Along with the Convention, in Strasbourg on January 28, 2005, the Supplementary Protocol on the prohibition of acts of a racist and xenophobic nature committed through computer systems was adopted. Its importance is also reflected in the fact that countries that are not in Europe joined it, such as the USA, Canada, Japan, the Dominican Republic, Panama, Mauritius, Australia, Israel, Sri Lanka and the Republic of South Africa (Bejatović, 2012).

The issue of safety in the virtual space is partially regulated by other conventions that concern this matter, such as: the Convention on the Protection of Individual Rights in Relation to the Automatic Processing of Personal Data, the Convention on the Protection of Children from Sexual Exploitation and Sexual Abuse, and the Convention on the Prevention of Terrorism.

The United Nations also worked to connect countries. The various bodies of this organization, in accordance with their powers, acted in the direction of raising awareness and connecting members in opposing the threats posed by high-tech crime. Resolution no. 55/2 of the UN General Assembly of September 18, 2000, also known as the Millennium Declaration, lists the safe and accessible sharing of new technologies among the goals for the coming millennium. In addition, the General Assembly adopted a number of resolutions related to the fight against misuse of information technologies and international Internet security.

The task of harmonizing national legislation in the field of high-tech crime and security in cyberspace is assigned by the United Nations to the International Telecommunication Union (ITU), its agency for the issue of information and communication technologies (ICT). In May 2007, the ITU presented a document called A Global Cybersecurity Agenda (GCA) which outlined the main problem and recommendations for improving security.

Also, the Economic and Social Council of the United Nations, in July 2007, adopted Resolution 2007/20, which talks about international cooperation in the field of prevention, investigation, prosecution and punishment of economic crime and acts related to identity abuse.

Many other organizations, such as NATO, OSCD, OECD, ICANN, AU, ASEAN, OA, have dealt with solving the problems of high-tech crime and threats to modern society with their internal documents (Pernik, 2014).

The objectives of the work and the methodology used

The aim of the paper is to answer the question of what are the legal aspects of the fight against high-tech crime in the European Union (EU), because the fight against high-tech crime includes various areas, factors and aspects. In order to answer that question, it was necessary to define the basic terms, collect data through research, classify and analyze them. In that process, three basic questions arose:

1. What are the documents of the European Union that govern the legal aspects of the fight against high-tech crime?
2. How is it arranged?
3. To what extent is the domestic legal system harmonized with the European one?

Scientific research is the initial step by which existing knowledge is verified and new knowledge is acquired, because the description of previous activities is the first step in which the initial state is completely, objectively and systematically determined, that is, the facts are established, while the analytical method was used to determine their mutual conditioning and reveal new facts, their relations or consequences. Content analysis implies research and consideration of a large number of legal sources, bearing in mind the various bodies of the Union and their powers to enact binding acts as well as documents which, although not binding, have significance for the creation of the policy of the Union and its members. In addition to acts adopted by its bodies, the European Union signs and accedes to international agreements adopted under the auspices of other international organizations, primarily the United Nations and the Council of Europe. All these rules form the legal framework for the fight against high-tech crime. In this sense, for the purposes of writing this paper, the following texts were analyzed:

- Communiqué on creating a safer information society by improving the security of information infrastructure and combating computer crime, (COM (2000) 890 final)
- Framework Decision on combating fraud and counterfeiting of non-cash means of payment, 2001/413/JHA
- Communication on Network and Information Security: Proposal for an EU Policy Approach (COM(2001)298 final)
- Communication on a strategy for a secure information society (COM (2006)251 final)
- Communication on combating spam, spyware and malware (COM (2006)688 final)
- Regulation EU/460/2004 establishing the European Network and Information Security Agency (ENISA)
- EU Framework Decision 2005/222/JHA on attacks on information systems,

- Directive 2002/58/EC on the processing of personal data and protection of privacy in the electronic communications sector,
- Decision 2001/413/JHA on the fight against fraud and counterfeiting of non-cash means of payment,
- EU Framework Decision 2004/68/JHA on the sexual exploitation of children and child pornography in relation to child pornography published using information systems
- EU Framework Decision 2008/913/JHA Decision on the fight against racism and xenophobia,
- Directive 2006/24/EC on the retention of data in connection with the provision of public electronic communication services,
- Framework Decision 2005/222/JHA on attacks on information systems,
- European Security Strategy "The European Internal Security Strategy in Action: Five Steps to a Safer Europe",
- Directive 2013/40/EU on attacks on information systems,
- European Security Strategy "A Safer Europe in a Better World"
- Proposal for a Regulation on ensuring access to and preservation of evidence COM(2018) 225 final- 2018/0108(COD) and
- Proposal for the Directive on the appointment of legal representatives COM/2018/226 final - 2018/0107 (COD),
- Directive EU/ 019/713 about the fight against fraud and the facsification of non-cash means of payment
- Regulation EU/2019/881 on ENISA (European Agency for Cyber Security) and information and communication technologies on cyber security certification and amendments to Regulation EU/526/2013.

After determining the starting points, classification of data according to nature or properties was started. The synthesis of the collected knowledge and the presentation of the research results are given in the form of the conclusion that the Union, in accordance with its powers, is working to create a coherent legal framework that obliges various actors to act.

Results of work with discussion

The development of the information society and new technologies have contributed to competitiveness, economic growth and easier employment within the Union, but they have also exposed legal and natural persons to the risk of cyber attacks. And, while the Council of Europe and the United Nations worked rapidly to define high-tech crime and develop a methodology to combat it, the European Union did not show any interest in this area, as if it was waiting to see the outcome of the activities that took place under the auspices of the aforementioned two organizations. It is only later that it begins to adopt legislation that has as its theme the fight against high-tech crime. Over time, the work of the EU to regulate the framework for the safe use of computers and

virtual space is becoming more and more important because a safe Internet space is of key importance for the functioning and development of the internal market (De Hert et al, 2006). The basis for this is found in Article 16 of the Treaty on the Formation of the EU (TFEU), also known as the Treaty of Lisbon, which introduces a special legal basis for the adoption of rules related to the protection of individuals with regard to the processing of personal data by the institutions of the Union, by the states member states when performing activities that fall within the scope of Union law, and the rules relating to the free movement of such data. Since the Union has above all a political-economic character, its basic areas of action are the cooperation of police and judicial bodies in that fight and the development of international cooperation, but also the adoption of domestic legal norms in the member states that will create adequate and effective legal instruments for combating cybercrime, which will be applicable, rational, efficient and fair (Bejatović, 2012).

The first document adopted in 2001, entitled "Communiqué on the creation of a safer information society by improving the security of information infrastructure and combating computer crime", proposes cooperation in many areas, and in particular the amendment of the legislation, which would cover high-tech crimes and harmonize the criminal policy of the members regarding those actions, as well as mutual recognition of pronounced judgments. This was an important, first step, because until then, criminal offenses related to high-tech crime did not exist in many countries. The importance of the cooperation of all interested parties in the collection and preservation of evidence was also mentioned, because it is not an issue that only concerns the judicial authorities, but also the economy and individuals. The communiqué set in this way led to the initiation of a series of activities and the adoption of new documents, the first of which was the Framework Decision on the fight against fraud and the fasification of non-cash means of payment, which protected all payments within the Union.

The EU Agency for the Cooperation of Judicial Institutions of the Member States in Criminal Matters (EUROJUST) was established to fight against cross-border crime and organized criminal groups. As part of the mandate of EUROJUST, a unit for cooperation between prosecutor's offices was established to combat various forms of crime, including cybercrime. An agreement was reached on the issuance of the European Arrest Warrant (EAW). The mechanism for issuing and responding to the European arrest warrant is one of the most important instruments that accelerates and enhances European judicial cooperation. Among the crimes for which an EAW can be issued are cybercrime, fraud during non-cash payments and forgery (Wennerström, 2010).

The Communication on Network and Information Security (COM (2001)298 final) is the first formulated proposal for EU policy. Cybersecurity policy has since been developed through a series of actions, representing a strategy for a

secure information society, combating spam, spyware and malware and leading to the creation of the European Network Security Agency (ENISA) in 2004. In addition to the concrete solutions that were offered for the observed problems, the importance of these activities was in raising awareness of the importance of Internet security problems, cooperation and more responsible use of information technologies. The communications were the basis for the adoption of new documents that were created to prevent the commission of the act or to prevent the occurrence of significant consequences.

EU Framework Decision 2005/222/JHA on attacks on information systems of February 24, 2005 sets as its main goal the improvement of cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services, through the convergence of national rules of criminal law in areas of attacks on information systems. The decision provided for a deadline of two years for its implementation, thus highlighting the urgency in the actions of the competent authorities of the member states in order to improve cooperation and begin to exchange all relevant information and establish operational contact points that work non-stop. It represents an attempt to overcome significant gaps and differences in national laws, which hindered police and judicial cooperation in the fight against organized crime and terrorism. The decision follows the approach taken by the Council of Europe Convention, and requires EU member states to criminalize intentional, illegal access to information systems, illegal interference with the system and illegal downloading of data. Such acts must be punished by effective, proportionate and dissuasive criminal penalties, and a criminal offense in the context of a criminal organization, which causes significant loss or affects important interests, must be considered an aggravating circumstance.

The EU addressed spam for the first time in its Directive 2002/58/EC on privacy and electronic communications relating to the processing of personal data and the protection of privacy in the electronic communications sector, stating that the single market requires a harmonized approach in this area because the volume of spam mail can cause difficulties for electronic communication networks and equipment. In doing so, it is not relevant whether subscribers of websites or electronic bulletin boards are violated by unsolicited communication for direct marketing purposes, by means of automated calling machines, faxes and e-mails, or SMS messages. In parallel with data protection and the fight against fraud and counterfeiting of non-cash means of payment, the European Union fights against sexual exploitation of children and child pornography published using information systems and against any form of racism and xenophobia.

This was followed by the adoption of several recommendations to the members in different forms, the most significant of which was Directive 2006/24/EC on the retention of data in connection with the provision of public electronic

communication services and amendments to Directive 2002/58/EC, which was an important step towards the establishment of a harmonized system for the collection and storage of traffic data in the EU, and Framework Decision 2005/222/JHA on attacks on information systems. The directive was adopted on the basis of the conclusions of the Council for Justice and Internal Affairs of December 19, 2002, in which it was particularly emphasized that, due to the significant growth of opportunities provided by electronic communications, data related to the use of electronic communications is a valuable tool in prevention, investigation, detection and prosecution of criminal acts, especially organized crime. The Framework Decision, on the other hand, was an attempt by the European Union to achieve a minimum level of convergence with regard to three computer crimes (illegal access to information systems, illegal interference of systems, illegal interference of data), the definitions of which are largely based on those of the Council Convention of Europe on cybercrime. However, it is surprising that the Framework Decision did not reach a higher level of convergence than the Council of Europe Convention in terms of applicable sanctions. Article 6 of the Framework Decision foresees a series of "minimum-maximum" sanctions, which for illegal interference of the system and illegal interference of data must be between 1 and 3 years in prison. Member States were asked to implement these provisions by the end of 2007. Despite various documents and attempts to create a coherent system that would make it easier for members to connect, cooperate and harmonize activities in protecting individuals, companies and institutions from cyber attacks, significant results were absent due to the structure and organization of the European Community. With the adoption of the Treaty on the Functioning of the European Union (Lisbon Treaty - UFEU), the Union was given new powers and opportunities to act in the field of internal security. Immediately after the entry into force of the Lisbon Treaty, the Stockholm Program was adopted in 2009 and the Internal Security Strategy in early 2010 (Nikodinovska-Stefanovska, Đurovski, 2012). At the end of 2010, the European Commission, in cooperation with the European Parliament and the Council of the European Union, produced a document entitled "European internal security strategy in action: five steps towards a safer Europe", stating that the cyberspace security system has five strategic priorities: achieving elasticity, in the sense that systems automatically return to a normal state after an incident, a significant reduction in cybercrime, the development of a cyber defense policy and capabilities compliant with the Common Security and Defense Policy (CSDP), the development of industrial and technological resources for cyber security and *the* establishment related international cyber security policies for the Union and promoting the fundamental values of the European Union.

The most ambitious EU instrument adopted during that period is the Directive on attacks on information systems (2013/40/EU) of August 12, 2013, which strengthens network and information security (NIS) and introduces the obligation

to report incidents for the private sector (including operators basic services and digital services). The directive prescribes measures to ensure a high common level of network and information security throughout the Union, which requires member states to develop a national strategy for network and information security (NIS), as well as a cooperation plan that enables the implementation of NIS. The members are obliged to form expert national teams, first of all a team responsible for computer incidents (Computer Emergency Response Team - CERT), which upon establishment cooperate with police agencies on the prevention, detection and response to cyber attacks, but also with the task of developing national plans for unforeseen situations. CERT-EU was established for EU institutions in 2012. The European information sharing and alert system (EISAS) is being developed as a network of contacts between members and other relevant bodies. In the member states, National Competent Authorities are formed, as the most important domestic institutions with the task of monitoring the implementation of the Directive at the national level and cooperating with the same bodies of other member states, security services and data protection bodies, as well as acting on received notifications of incidents that they are instructed by the public administration and public operators of telecommunication and information services. In addition to the two basic bodies, each member state can form: the Information Security Authority (IAA), the TEMPEST Authority (TA), the Cryptographic Solution Approval Authority (CAA) and the Cryptographic Material Distribution Authority (CDA).

The national security strategy represents the general programmatic standpoint of a state in the area of its security (Nedeljković, Forca, 2018). The EU adopted the European security strategy "A safer Europe in a better world" (A safer Europe in a better world, European security strategy) in 2013 with the aim of strengthening the cyber security of public administration and critical infrastructure, in which it emphasizes the need for the development of a strategic culture for early and quick interventions in situations where security is threatened in any way. The strategy has three chapters: analysis of the security environment, in which global challenges and key threats are presented; defining strategic goals and assessing political implications for Europe and aimed at fighting high-tech crime by focusing on partnership with the economy and building capacity within member states to counter cyber attacks (Carrapico, Barinha, 2018). In 2013, within the framework of the existing structures of EUROPOL, the Union established the Criminal Center for High Technologies (E/C3), through which member states and institutions of the Union build and improve operational and analytical capacities for conducting investigations and cooperation with international partners. The center cooperates with the European Network and Information Security Agency (ENISA) as well as the network of national teams for computer incidents (CERTs). The European Agency for Network and Information Security (ENISA) was established in 2004 by Regulation of the European Commission and the

Council No. EC/460/2004 with a limited mandate that has been extended since that day. In April 2019, a new Regulation was adopted renaming ENISA to the European Cyber Security Agency and giving it new powers and adding new bodies. The headquarters of the Agency is in Athens, it has the status of a legal entity, and it is financed from funds from the European Union budget, funds from third countries that participate in the work of the Agency, as well as donations from member states in money or in kind. The original task of ENISA to carry out tasks for the purpose of establishing a high level of network and data security in the European Union, raising awareness of information security and developing and promoting a culture of network and data security for the benefit of citizens, consumers, businesses and public authorities of the European Union has been expanded in terms of cyber certification security. In each of the member states, ENISA has the widest legal capacity that legal entities have under the internal law of the member state and can conclude contracts in accordance with the law that applies to the specific contractual relationship. It is authorized to cooperate with third countries and international organizations in order to promote international cooperation in the field of network and data security. The bodies of ENISA are: Management Board, Executive Board, Executive Director, Permanent Body of Stakeholders (which includes representatives of the academic community, business and consumers) and ad hoc working groups. Since 2019, there is also a permanent body of National Liaison Officers, and ENISA is responsible for the cybersecurity certification scheme for products, services and processes to support the Digital Single Market.. The European Parliament, the Council, the European Commission and the competent regulatory bodies of the Member States can submit requests for advice and support.

The Council of the European Union, in June 2017, approved the Cyber Diplomacy Toolkit with the ultimate goal of strengthening EU activities and enhancing a coordinated response in case of cyber attacks against European targets. The most important actors in this area, according to that set, are: the European Network and Information Security Agency (ENISA), the European Police Office (EUROPOL) including the European Cybercrime Center (E/C3) and the European Defense Agency (EDA). The European Commission, the EU's executive body, is involved in the formulation of the Union's cyber security policy, priorities and objectives through the Directorate General for Home Affairs (DG Home) which is responsible for police and criminal justice cooperation and oversees the activities of Europol, while its part is in charge of DG Connect for the protection of critical infrastructure and supervises the activities of ENISA. The EDA is in charge of further developing the EU's cyber capabilities together with the EU Military Staff (EUMS). The Judicial Cooperation Unit (EUROJUST) has a role in the fight against cybercrime by facilitating cooperation between prosecutors. The two-year project COURAGE (Cybercrime and Cyberterrorism European Research Agenda) from the EU's Seventh Framework Program delivered a comprehensive research

agenda and coordinated roadmap based on collaboration with 17 organizations from 12 European countries on the ground. The final results of the project published in May 2016 identified missing solutions for better application of existing rules and recommended their correction (Jerman-Blažič et al, 2016).

In 2018 the European Commission presented the basis for two sets of negotiations, with the United States (USA) and for the Second Additional Protocol to the "Budapest" Convention of the Council of Europe on cybercrime. Both documents provide for strong data protection and privacy measures, and concern the provision of cross-border access to electronic evidence in criminal investigations. In the negotiations with the USA, it is proposed to introduce a binding European production order and a European evidence preservation order. Both orders must be issued or certified by a judicial authority of the Member State. An order may be issued to request the retention or production of data stored by a service provider located in another country, which is required as evidence in criminal investigations or proceedings. The second act introduces the obligation for service providers to appoint a legal representative in the Union who will ensure the reception, compliance and execution of decisions so that competent national bodies can collect evidence in criminal proceedings. The resulting reduction of obstacles would ensure better functioning of the internal market in a manner consistent with the development of the common area of freedom, security and justice.

A significant step forward in the fight against cybercrime is Directive 2019/713/EU on fraud in non-cash payments, which updates the legal framework, removes obstacles to operational cooperation and increases prevention and assistance to victims, in order to actions to enforce the law against fraud and forgery of non-cash means of payment were more effective. The last in a series of acts related to internet security is the Temporary Regulation for regulating the processing of personal and other data with the aim of combating sexual abuse of children from September 10, 2020, created on the basis of Directive 2002/58/EC.

The Republic of Serbia adopted the Law on the Organization and Competence of State Authorities for the Fight against High-Tech Crime (VTK Law) in 2005, which established an institutional framework for the fight against cybercrime, as the Law provided for the formation of a specialized unit of the Ministry of Interior, as well as special judicial and prosecutorial bodies. for the fight against high-tech crime, the Special Prosecutor's Office for high-tech crime as part of the Higher Public Prosecutor's Office in Belgrade, the High Court as a first-instance court, and the Court of Appeal in Belgrade as a second-instance judicial body. The law was passed after the adoption of the Budapest Convention and the Additional Protocol was harmonized with them, which started the application of international standards important for this area. The Criminal Code of the Republic of Serbia, adopted in 2005, introduces computer crimes into the legal system. At

the beginning of 2009, the National Assembly of the Republic of Serbia ratified the Budapest Convention and the Additional Protocol by means of special laws, but also adopted new and supplemented the existing legal and by-laws of importance. In the screening report for Chapter 24 "Justice, Freedom, Security" which was done in 2014, the European Commission found that Serbia is among the countries where the risk of cyber attacks is higher, which is why it is necessary to continue work on training competent bodies for combat against those attacks, but also on raising users' awareness of the risks they are exposed to (Krivokapić, Petrovski, 2016).

The Law on Electronic Communications regulates for the first time the conditions and manner of performing activities in the field of electronic communications, the competence of state authorities, as well as the protection of the rights of users and subscribers, the security and integrity of electronic communication networks and services, the secrecy of electronic communications, the lawful interception and retention of data, as well as other issues of importance for the functioning and development of electronic communications in the Republic of Serbia. The law was adopted with the intention of protecting users' privacy from unauthorized access to their digital records and data from their profiles (Darijević, 2021).

In addition to legal and by-laws, the Information Society Development Strategy 2010 - 2020 was adopted and the Serious and Organized Crime Threat Assessment (SOCTA) was carried out in 2015. The assessment is a strategic document that considers various forms of serious and organized crime, including cybercrime, which provides the basis for the operational work of the police in accordance with existing trends (Krivokapić, Petrovski, 2016).

The Law on Information Security, which entered into force in February 2016, applies to legal entities. The establishment of institutions is prescribed, among which the most important is the National Center for the Prevention of Security Risks in ICT Systems, the domestic CERT team. He is entrusted with collecting information, classifying information about incidents and risks, raising awareness among citizens and cooperating with public and business entities (Đukić, 2018). After that, in March 2016, the Body for the Coordination of Information Security Affairs was established, with which the Republic of Serbia joined the network of national bodies for the exchange of information and the fight against crime, as prescribed by Directive 2013/40/EU.

Conclusion

Information security is defined as a set of measures that enable data handled through computer systems to be protected from unauthorized access, as well as to protect the integrity, availability, authenticity and non-repudiation of that data, so that the system functions as intended, when intended. and under the control of authorized persons. Since the EU, unlike some other organizations, does not have

the capacity to provide direct assistance to members under cyber attack, it acts as an intermediary to help share knowledge and experience and support the adoption of best practices for individual problems. The role that the EU has in terms of training, cooperation and connecting members in the fight against high-tech crime, as well as the private-public partnership that proves to be indispensable in the successful discovery, collection and preservation of evidence, which is the basic mode of action in the Union, increases the importance of the EU in the fight against cyber crime. Relying on the powers granted by the Treaty of Lisbon (TFEU), the Union systematically creates a unique legal framework that fully identifies those responsible for countering cyber attacks, harmonizes and complements the substantive and procedural criminal law of the members, and thus strengthens the internal security system of the Union as a whole.

Serbia has signed the Council of Europe Convention on Cybercrime and has largely harmonized its legislation with the 2013 Directive on Attacks on Information Systems. Amendments to the law are needed, especially in the part related to securing and collecting evidence and sanctions, so that the legislation is fully harmonized with EU regulations. In the Report on Serbia's progress in 2014 and 2015, the EU Commission pointed out that it is necessary to further harmonize the legal framework related to child pornography. One of the demands was the adoption of a strategy on high-tech crime. With the Action Plan for Chapter 24, the Government of Serbia has provided measures that will harmonize its laws with the legislation and standards of the European Union for the fight against high-tech crime through the analysis of the existing legal framework, the drafting of laws and other regulations based on the analysis in order to improve organizational, human and technical capacities authorities in charge of combating high-tech crime, and above all training of employees in the Special Public Prosecutor's Office and the police unit for high-tech crime. The action plan for Chapter 24 foresees additional specialized training in order to strengthen the capacities of state bodies responsible for the fight against high-tech crime. Within the High-tech Crime Department of the Ministry of Interior, specialized units for investigations of credit card abuse, internet commerce and internet banking and a unit for suppressing illegal and harmful content on the internet were established, which should contribute to better conducting investigations and gathering evidence. With the mentioned amendments to the legislation and the establishment of national bodies, Serbia has fulfilled the minimum conditions stipulated by the legal framework of the Union for combating cyber attacks.

In addition to expert bodies dealing with the detection and prosecution of perpetrators of criminal acts, cooperation between the private and public sectors, civil society organizations dealing with high-tech security and the fight against high-tech crime, and the academic community is necessary. Many countries are extremely slow and inadequately trained to respond to these threats, which can be remedied by better international exchange of experience and best practice in the

field of cyber security, which is facilitated by the adoption of a large number of multilateral agreements.

Literature

1. Bejatović S., 2012. High-tech crime and criminal legal instruments of opposition, Proceedings of the International Scientific Conference "Suppression of crime and European integration, with reference to high-tech crime", High School of Internal Affairs of the Republic of Srpska: 17-30 (available at: http:// education.muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)
2. Bjelajac Ž., A. Filipović. 2021. Specific characteristics of digital violence and digital crime, Law theory and practice (4): 16 – 32
3. Carrapico H., A. Barinha. 2018. European Union cyber security as an emerging research and policy field, Symposium: European Union cyber security as an emerging research and policy field, European Politics and Society, 19 (3): 299-303
4. Csonka P. 2006. The Council of Europe's Convention on cyber-crime and other European initiatives, Revue international de droit penal, 3-4 (77): 473 - 501
5. Darijević V. 2021. Cybercrime as a security risk on the Internet, Megatrend review, 2(18): 257-266
6. De Hert , P., G. González Fuster , BJ. Koops . 2006. Fighting cybercrime in the two Europes, The added value of the EU framework decision and the council of Europe Convention, Revue internationale de droit pénal 3-4 (77) : 503-524
7. Đukić A. 2018. Organized high-tech crime - concept, development and basic characteristics, Vojno delo (3):128-156
8. Jerman- Blažić, B., T. Klobučar, J. Stefan. 2016. Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda, European Intelligence and Security Informatics Conference (available on the website: https:// web.archive.org/web/20190223201002id_/http://pdfs.semanticscholar.org/4ca3/37b1bc74362b632095de1c40cf7c835498b7.pdf)
9. Krivokapić, D. and A. Petrovski. 2016. Cybercrime in Serbia before the opening of Chapter 24 (Justice, Freedom and Security), Share Foundation (available on the website: https://bezbednost.org/wp-content/uploads/2020/06/sajber_kriminal_u_srbiji_pred_otvaranje_poglavlja_.pdf)
10. Nedeljković, S. and B. Forca. 2015. European security strategy and cyber threats - significance for Serbia, Military Work 3: 135-155
11. Nikodinovska-Stefanovska, S. and M. Đurovski. 2012. Internal security of the EU and police cooperation in the post-Lisbon era, in Proceedings of the

International Scientific Conference "Suppression of Crime and European Integration, with a Focus on High-Tech Crime", High School of Internal Affairs of the Republic of Srpska: 385 - 395 (available at: http://education. muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)

12. Pernik, P. 2014. Improving Cyber Security: NATO and the EU International Center for Defense Studies (available on the website: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf)
13. Perović, M. 2018. Cybercrime as a global threat in the world, Vojno delo 3: 157-164
14. Romić, M. and N. Grbić-Pavlović. 2012. International legal documents governing the field of high-tech crime in the proceedings of the International Scientific Conference "Suppression of crime and European integration, with a focus on high-tech crime", High School of Internal Affairs of the Republic of Srpska: 193-217 (available at: http://education. muprs.org/wp-content/uploads/2014/12/Zbornik-Visokotehnoloski-kriminal.pdf)
15. Wennerström E. 2010. EU-legislation and Cybercrime: A Decade of European Legal Developments, Stockholm Institute for Scandian Law, 47-21: 452-472 (available on the website: https://scandinavianlaw.se/pdf/47-21.pdf)