*Катарина Арсић**

DOI: 10.51204/Zbornik_UMKP_24152A
Прегледни научни рад

САЈБЕР ПРОСТОР И МЕЂУНАРОДНО ПРАВО – АНАЛИЗА И ДОМАШАЈИ КОНВЕНЦИЈЕ САВЕТА ЕВРОПЕ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Апстракт: Сајбер простор и информационо-комуникационе технологије представљају важан сегмент 21. века, а високотехнолошки криминал и сајбер претње уопште један од важних изазова данашњице. У раду се анализирају главне карактеристике сајбер простора. Посебан акценат ставља се на Конвенцију Савета Европе о високотехнолошком криминалу (Будимпештанску конвенцију) као првом међународном уговору који инркимининше поједине радње на рачунарским системима. Ова конвенција која је потписана 2001. године, а ступила на снагу 2004. године, има за циљ да омогући хармонизацију прописа држава уговорница у области борбе против високотехнолошког криминала, али и да олакша међународну сарадњу у истрагама и кривичним поступцима. Кроз друге иницијативе на регионалном и глобалном нивоу, покушаћемо да одговоримо на питање у којој мери ова материја јесте регулисана међународним јавним правом, зашто је овај документ још увек актуелан и важан, а покушаћемо и да предвидимо у ком ће правцу даље тећи развој међународних правила по питању информационо-комуникационих технологија.

Кључне речи: сајбер простор, високотехнолошки криминал, информационо-комуникационе технологије, Будимпештанска конвенција, међународно јавно право, сајбер безбедност.

1. УВОД

Сајбер или високотехнолошки криминал јесте свакако један од актуелних али и нових безбедносних изазова. Имајући у виду да превазилази

* Студент докторских студија Универзитета у Београду – Правног факултета, katarina.arsic16@gmail.com.

границе суверених држава, како би му се државе адекватно супротставиле, али и како би га спречиле, потребно је да сарађују не само у оквиру постојећих међународних правила, већ и да унапреде сарадњу кроз нове модалитете и прописе у овој сфери. Циљ овог рада јесте да размотримо и анализирамо шта је то сајбер простор, како да боље схватимо сајбер безбедност и какве све претње високотехнолошки криминал доноси, али и који су то оквири сарадње између држава у овој области. Посебан акценат ће бити стављен на Конвенцију о високотехнолошком криминалу, која је донета у оквиру Савета Европе, као првог међународног уговора који инкриминише одређене радње на интернету и рачунарским мрежама, али и омогућује сарадњу држава уговорница у овој области, о чему ће касније бити речи. Затим ћемо покушати да евидентирамо мане и недостатке које критичари овог документа истичу и покушати да пронађемо одговор како их можемо спречити. На самом крају, анализираћемо прописе међународног јавног права који се могу односити на област информационо-комуникационих технологија, као и друге аспекте сарадње у овој сфери како на регионалном, тако и универзалном плану.

2. ДЕФИНИЦИЈЕ И СПЕЦИФИЧНОСТ САЈБЕР ПРОСТОРА И ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

Да бисмо могли да говоримо о Конвенцији о високотехнолошком криминалу, морамо пре тога дефинисати најважније термине. У литератури често наилазимо на термине попут сајбер простора, сајбер безбедности, информационо-комуникационих технологија, сајбер ратовања, сајбер напада и претњи, високотехнолошког криминала и др.

Сајбер простор не треба поистоветити са интернетом – сајбер простор чине информационе мреже које могу а не морају бити повезане на интернет. Говоримо пре свега о вештачкој творевини коју можемо посматрати као глобалну средину „обраде, размене, стварања и уништавања информација између умрежених информационих система, који омогућавају одговарајући протоколи и физичка основа".[1] Како се истиче, „највећи проблем сајбер напада јесте што је тешко одредити намеру, идентитет или политичку мотивацију нападача. Сајбер напади су постали моћна, нискобуџетна опција ратовања која материјално оштећује друге једноставним кликом на дугме. Сајбер напад служи као асиметрично оружје које омогућава инфериорним групама и државама да наносе штету технолошки и војно супериорним непријатељима."[2] Рат у сајбер сфери сматра се трећом врстом сукоба, поред

1 Д. Младеновић *et al.*, „Дефинисање сајбер ратовања", *Војнотехнички гласник*, LX, (2)/2012, 91–92.

2 З. Јефтић *et al.*, „Савремени конфликти и њихове тенденције", *Војно дело*, 7/2018, 37.

међународних сукоба, односно сукоба са великим силама и грађанског рата, а главна средства ратовања јесу лаптопови, модеми, телефони и други електронски уређаји.[3] Овде треба нагласити да не постоји опште прихваћена дефиниција сајбер простора. Као што смо претходно навели, можемо рећи да је то вештачка творевина која означава свет рачунарских мрежа и дигитални свет уопште и представља окружење у коме лица комуницирају уз помоћ умрежених рачунара. Он је резултат како друштвених потреба, тако и технолошких иновација.[4] Као што можемо да видимо, сајбер простор није нужно лоша ствар, лоше је кад почне да се користи за извршење кривичних дела или било какве друге врсте претњи.

Сајбер претње превазилазе државне границе, усложњавају и повезују активности. Самим тим, говоримо, између осталог, о политичком, безбедносном, али и питању од националног интереса. Оне су нарочито порасле током пандемије COVID-19 а и данас остају актуелна тема.[5]

Сајбер напад представља напад на сајбер простор са циљем да рачунарску инфраструктуру омете, онемогући њен рад, уништи, контролише или злоупотреби податке и информације које се налазе на мрежи.[6] У литератури не постоји сагласност до које мере ове претње могу угрозити не само појединце већ и државе, тако да постоје аутори који сматрају да се поједине врсте сајбер напада могу подвести под агресију, те стога државе на такве акције могу одговорити правом на самоодбрану. Сајбер напади сматрају се једним аспектом хибридних претњи, које представљају комбинацију не само претњи конвенционалним оружјем, већ и претњу невојним средствима у које спадају разне економске мере, психолошке, али и сајбер операције. Премда се не уклапа у општеприхваћену дефиницију агресије из 1974. године која за постојање агресије поставља услов примене оружане силе, постоје аутори, попут на пример, Коха који сматрају да би се одређене радње у сајбер простору које би за последицу имале смрт, повреде или пак значајније последице могу бити посматране као употреба силе. Наведено питање је посебно осетљиво имајући у виду прекогранични карактер сајбер претњи, а мере које се предузимају могу се злоупотребити, али и тумачити као мешање у унутрашње

3 *ibid.*, 39; S. Shackelford, „From Nuclear Warto Net War: Analogizing Cyber Attack in International Law", *Berkeley Journal of International Law*, 27, 1/2008, 200.

4 Д. Вулетић, „Употреба сајбер простора у контексту хибридног ратовања", *Војно дело*, 7/2017, 310.

5 Д. Вулетић, Б. Ђорђевић, „Проблеми и изазови управљања интернетом на међународном нивоу", *Међународни проблеми*, LXXIII, 2/2021, 236; Н. Радић, „Сајбер безбедност и потреба промене модела праћења превара и финансијског криминала", *Трендови у пословању*, 8, 16/2020, 87; N. Katagiri, „Why international law and norms do little in preventing non-state cyber attacks", *Journal of Cybersecurity*, 2021, 1–2.

6 С. Цветковски, В. Кенко, „Свеобухватни приступ НАТО-а сајбер одбрани", *Криминалистичке теме*, 19, 5/2019, 506; B. Walton, „Duties Owed: Law-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law", *The Yale Law Journal*, 126, 5/2017, 1466.

ствари држава, или пак као контрола интернета, медија и информационо-комуникационих технологија. Највећи број самих сајбер напада, односи се на сајбер криминал тако да тешко да се изоловани напади на информациони систем може сматрати агресијом и поводом за самоодбрану.[7]

Без обзира на то, чињеница да ће активности ићи у прилог унапређења правила по питању забране употребе силе и сајбер напада, као и настанку правила у случају потенцијалног сајбер конфликта говори податак да је у оквиру НАТО, 2013. године донет Талински приручник о међународном праву који се примењује на сајбер ратовање. Међутим, имајући у виду класично схватање агресије као употребе оружане силе, сајбер напади ниског интензитета не могу се тумачити као агресија.[8] Наведени приручник ослања се на Предлог чланова о одговорности држава за међународно противправне акте које је израдила Комисија за међународно право. Дакле, односи се највише на одговорност државе за сајбер нападе, али не искључује одговорност државе за радње приватних лица ако се докаже да су та приватна лица радила у складу са инструкцијама, директивом и контролом државе. Заправо, Талински приручник прописује да државе морају да се уздрже од тога да дозволе да интернет инфраструктура на њиховој територији и која је под њиховом контролом буде коришћена према другим државама за неповољне и противправне радње, а уколико се такав напад догоди, дозвољава и контра мере. Међутим, не може се у потпуности направити оваква аналогија, имајући у виду да није увек лако утврдити да иза неког сајбер напада од стране недржавног актера стоји држава, али и лоцирати групу људи или лице које је у некој другој држави учинило сајбер напад. Нарочито је компликована ситуација када се напад изводи посредством друге државе, као што је тешко утврдити и одговорност друге државе за сајбер напад. Дакле, закључујемо да не постоји сагласност о применљивости и важењу међународног јавног права у овој области,[9] односно да тек треба да видимо у ком ће правцу тећи развој сајбер правила.

Сајбер криминал се дефинише као злочин учињен на рачунару, према рачунарском систему и корисницима, али може бити и било које друго

7 Д. Вулетић, *op. cit.*, 309, 312 и 317–318; R. Titriga, „Cyber-attacks and International law of armed conflicts; a „jus ad belum" perspective", *Journal of International Commertional Law and Technology*, 8, 3/2013, 182–183; Д. Младеновић, М. Дракулић, Д. Јовановић, „Неутралност и сајбер ратовање", *Војно дело*, 63, 3/2011, 198.

8 B. Walton, *op. cit.*, 1470, 1472; K. Mačak, „Is the International Law of Cyber Security in Crisis?", *8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2016, 134.

9 P. Margulies, „Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *Melbourne Journal of International Law*, 14/2013, 2–5, 9; S. Shackelford, *op. cit.*, 195; Ж. Новичић, „Нова стратегија сајбер безбедности ЕУ за дигиталну деценију – анализа", *Развојни правци Европске уније након пандемије COVID 19* (ур. Н. Станковић, Д. Дабић, Г. Бандов), Институт за међународну политику и привреду, Београд, 2021, 127; M. Schmitt, „"Below the treshold" cyber operations: the countermeasures response option and International law", *Virginia Journal of International Law*, 54, 3/2014, 706–707.

традиционално кривично дело учињено уз помоћ рачунара. Треба напоменути да не постоји ни општеприхваћена дефиниција сајбер криминала. Свакако можемо рећи да су у питању противзаконите или недозвољене активности које се спроводе преко глобалних електронских мрежа.[10] Као специфична кривична дела учињена на рачунару и интернету, она се могу односити на промену података, улазак у неауторизоване инструкције, коришћење неауторизованог процеса, али и крађу трансакција или промену и брисање складиштених података,[11] што ствара не само штету, него и страх код корисника интернета. У том смислу, већ се говори о сајбер криминологији као дисциплини која изучава узроке злочина који се дешавају у сајбер простору и његовог утицаја у физичком простору.[12] Сајбер безбедност самим тим представља технологије, процесе и праксе, који имају за циљ заштиту мрежа, рачунара, програма и података од напада, оштећења или пак неовлашћеног приступа.[13]

Без обзира на то што постоје ставови да је високотехнолошки криминал метод који се користи прекогранично као средство ратовања или дестабилизације,[14] а имајући у виду да се сајбер напади често дешавају на међународном нивоу, јер кривично дело у информационо-комуникационим технологијама може бити учињено од стране лица у једној држави, применом ресурса у другој држави, а да се у трећој држави налази жртва, с обзиром на карактер међународног права и непостојања централног тела,[15] у овом раду ће акценат бити на оним аспектима који се односе на Будимпештанску конвенцију о високотехнолошком криминалу.

3. КОНВЕНЦИЈА О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Када говоримо о улози и важности Конвенције о високотехнолошком криминалу, треба истаћи да она представља обавезујући документ за државе које су га прихватиле по питању сарадње у области високотехнолошког криминала. Како се истиче, говоримо о првом међународном уговору који,

10 D. Bunga, „Legal Response to Cybercrime in Global and National Dimensions", *Padjadjaran Journal*, 6, 1/2019, 70; M. Grotto, „Council of Europe Convention on Cybercrime and its ratification in the Italian Legal System", *Sistema Penal & Violência, Porto Alegre,* 2, 1/2010, 2.

11 D. Agung, „The Role of Interpol in the Settlement of Cybercrime Cases Under the Budapest Convention on Cybercrime", *International Journal of Global Community*, 5, 1/2022, 50.

12 И. Балтезаревић, Д. Танчић, „Утицај дигиталног окружења на ширење сајбертероризма", *Баштина*, 32, 57/2022, 159.

13 С. Цветковски, В. Кенко, *op. cit.*, 505.

14 M. Tennis, „A United nations Convention on Cybercrime", *Capital University Law Review*, 48, 2/2020, 191.

15 M. Keyser, „The Council of Europe Convention on Cybercrime", *J. Transnational Law and Policy*, 12/2003, 294; Д. Младеновић *et al.*, *op. cit.*, 93.

пре свега, обавезује државе уговорнице да хармонизију своје законе у области високотехнолошког криминала, али и омогућује интензивирање међународне сарадње у кривичним стварима. Конвенција има улогу да пружи свеобухватан одговор на кривична дела високотехнолошког криминала, али и обезбеди међународну сарадњу када и ако се она догоде.[16] Другим речима, улога ове конвенције је да обезбеди и олакша креирање униформног домаћег права држава потписница у области високотехнолошког криминала, односно кривичних дела учињених на интернету и другим мрежама попут угрожавања ауторских права, кривичних дела на рачунару, дечје порнографије или повреда безбедности мреже. Дакле, она пружа смернице државама како да своја национална законодавства хармонизују у овој области и олакшају међународну сарадњу. [17]

Конвенција је донета 2001. године у Будимпешти (зато се често користи назив Будимпештанска конвенција) са приоритетом да се успостави заједничко деловање у области криминалистике, пре свега у погледу заштите друштва од високотехнолошког криминала. Иако је усвојена у оквиру Савета Европе, овај документ има ширу територијалну примену, имајући у виду да су је усвојиле и ратификовале и државе које нису чланице ове међународне организације а учествовале су у преговорима попут Канаде, Јапана и Сједињених Америчких Држава. Колико је државама уговорницама било стало да се донесе правно обавезујући документ који би учврстио сарадњу између држава у овој области, говори чињеница да је за ступање уговора на снагу била довољна ратификација од стране минимум пет држава, од којих су три чланице Савета Европе и то се догодило 2004. године. Иако на први поглед она има ограничено територијално дејство имајући у виду да је отворена потписивање и прихватање од стране држава чланица Савета Европе, држава које нису чланице а учествовале су у преговорима, као и за државе којима се упути позив да је прихвате, данас међу 70 уговорних страна налазе се државе Азије, Блиског истока (Израел) Африке, али и Јужне Америке. Конвенцију је прихватила и Аустралија.[18] Такође, конвенција има два

16 M. Vatis, „The Council of Europe Convention on Cybercrime", Proceedings of a Workshop on Deterring cyberattacks, Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; *National Academic Press,* Washington D.C., 2010, 207; R. Titriga, *op. cit.*, 180; M. Tennis, *op. cit.*, 199; J. Clough, „A world of difference: the Budapest Convention on Cybercrime and the Challenges of Harmonisation", *Monash University Law Review*, 40, 3/2014, 698, 701.

17 C. DeLuca, „The Need for International Laws of War to Include Cyber Attacks Involving State and Non-state Actors", *Pace University Scholl of Law*, 3, 9/2013, 308; M. Grotto, *op.cit.*, 5; D. Bunga, *op. cit*., 72; Ж. Новичић, *op. cit.*, 125.

18 M. Tennis, *op. cit*., 200; D. Agung, *op. cit*., 51; C. DeLuca, *op. cit*., 307; Закон о потврђивању Конвенције о високотехнолошком криминалу, *Службени гласник РС – Међународни уговори, бр. 19/2009*; M.A. Vatis, *op. cit.*, 207, 220; M. Keyser, *op. cit*., 296–297; Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, 14. април 2024.

протокола, а први јесте Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичке природе извршених преко рачунарских система. Протокол је потписан 2003., а ступио на снагу 2006. године. Ратификовало га је 35 држава.[19] За потребе овог протокола „расистички или ксенофобни материјал означава сваки писани материјал, сваку слику или свако друго представљање идеја или теорија које заговарају, промовишу или подстрекавају мржњу, дискриминацију или насиље, против било којег појединца или групе појединаца, засновано на раси, боји коже, наследном, националном или етничком пореклу, као и вери, ако се користе као изговор за било који од тих фактора."[20] Други додатни протокол уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа потписан је у мају 2022. године и још увек није ступио на снагу имајући у виду да је за то потребно ратификација од минимум пет држава потписница што се још увек није догодило. Он прописује, између осталог, остваривање сарадње и комуникације са пружаоцима услуга на територији друге државе уговорнице у циљу откривања података о претплатнику у сврху кривичноправних истрага и поступака.[21]

Марко Грото идентификује три циља Конвенције. Први јесте да омогући хармонизацију правних прописа на националном нивоу држава уговорница, пре свега обезбеђивањем заједничке дефиниције одређених кривичних дела. Други циљ јесте дефинисање заједничких истрага и омогућавање кривичних процедура између чланица. И трећи циљ, омогућава међународну сарадњу између држава захваљујући сарадњи у кривичним стварима и истрагама захваљујући сталним контактима. То значи да државе морају да усвоје концепте сагласне Конвенцији, односно морају да садрже истоветне модалитете сарадње. За то је неопходно успоставити минимални заједнички стандард.[22]

Ова конвенција обавезује уговорне стране да усвоје пре свега законодавне, али и друге мере које су неопходне а у циљу успостављања кривичних дела у унутрашњем праву, која би била учињена у намери. Међутим, шта је намера, остављено је државама уговорницама да саме интерпретирају.

---

19 M. Vatis, *op. cit.*, 210; Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 189, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189, 14. април 2024.

20 Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичке природе извршених преко рачунарских система, *Службени гласник РС – Међународни уговори*, 19/2009.

21 Ратификовале су само Република Србија и Јапан. Погледати: Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 224, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, 14. април 2024. и Закон о потврђивању Другог додатног протокола уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа, *Службени гласник РС – Међународни уговори*, бр. 7 од 28.12.2022.

22 M. Grotto, *op. cit.*, 5; M. Keyser, *op. cit.*, 299

У Конвенцији се наглашава да страна уговорница може да услови да је кршењем мера безбедности дело учињено са намером прибављања рачунарских података или пак са неком другом нечасном намером.[23]

Оно што свакако можемо препознати из преамбуле јесте да је потребно да се правно обавезујућим документом униформишу прописи о заштити људи у сајбер простору и обезбеди међународна сарадња, да су државе уговорнице истакле свест да су континуирана дигитализација и глобализација компјутерских мрежа довели до фундаменталних промена, али и забринутост да би се рачунарске мреже и електронске информације могле злоупотребити и искористити за извршење кривичних дела. Додаје се да је потребно успоставити сарадњу између држава и приватног сектора, као и да је потребно остварити ефекте одвраћања за евентуалне учиниоце кривичних дела у сајбер простору, како на унутрашњем тако и на међународном плану.[24]

Треба нагласити да саму дефиницију високотехнолошког криминала ова конвенција не нуди. Она нуди дефиниције других појмова преко којих би се вршила кривична дела попут рачунарског система, рачунарског податка, давалаца услуге, али и података у саобраћају.[25] Међутим, осим што нуди модалитете сарадње, овај документ је важан јер прописује активности и радње које чине кривична дела у информационо-комуникационим технологијама. Кривична дела која она прописује можемо поделити у четири категорије: дела против поверљивости, целовитости и доступности рачунарских података и система, дела у вези са рачунарима, дела у вези са садржајем и дела у вези са кршењем ауторских и сродних права.[26] На пример, овај документ инкриминише незаконит приступ рачунарском систему у целини или његовом делу, незаконито пресретање преноса рачунарских података који нису јавне природе, противправно оштећење, брисање, погоршање, мењање или прикривање рачунарских података (или једном речју ометање података), противправно озмиљно ометање рада рачунарског система уношењем, преношењем, оштећењем, брисањем, погоршањем, мењањем или прикривањем рачунарских података (или ометање система), злоупотребу уређаја. Наведена дела спадају у прву категорију. У другу спадају фалсификовање у вези са рачунарима и превара у вези са рачунарима. У трећу групу можемо убројати кривична дела, односно радње у вези са дечијом порнографијом. За четврту категорију смо већ рекли да обухвата кршење ауторских и сродних права. Две ствари је овде неопходно напоменути. Прва да је држава уговорница дужна да предузме законодавне и друге мере како би наведене радње и активности биле прописане као кривична

23 M. Vatis, *op. cit.*, 210; M. Keyser, *op. cit.*, 299; Закон о потврђивању Конвенције о Високотехнолошком криминалу.

24 D. Bunga, *op. cit.*, 76–77; Закон о потврђивању Конвенције о високотехнолошком криминалу.

25 D. Bunga, *op. cit.*, 77; Закон о потврђивању Конвенције о високотехнолошком криминалу.

26 J. Clough, *op. cit.*, 702; M. Grotto, *op. cit.*, 5; M. Keyser, *op. cit.*, 297.

дела у домаћем законодавству. Друга напомена јесте да је битан услов да ова дела буду учињена са намером.[27] Једном речју, Конвенција настоји да одређена понашања која чине традиционална кривична дела инкриминише уколико се учине посредством нових технологија и како би лице које их је учинило било санкционисано.[28]

Конвенција захтева од држава уговорница да врши јурисдикцију за сва кривична дела учињена на њеној територији, броду или ваздухоплову који су регистровани сходно законима те државе. Такође, имаће надлежност и ако је кривично дело извршено од стране њеног држављанина, али и ако је дело кажњиво према прописима кривичног закона земље где је извршено, или пак ако је извршено на месту на коме ни једна држава нема надлежност.[29]

Поред обавезе да државе уговорнице инкриминишу и обезбеде санкције за одређена кривична дела, ова Конвенција садржи и одредбе које се односе на међународну сарадњу. Овај документ прописује међусобну сарадњу у најширем могућем обиму. Она се може остварити применом одговарајућих међународних инструмената кроз сарадњу у кривичним стварима, са циљем истрага или поступака који се односе на кривична дела у вези са рачунарским системима и подацима, а може бити и у сврху прикупљања доказа у електронском облику о кривичном делу.[30]

Ова конвенција прописује екстрадицију – под условом да је у питању кривично дело кажњиво у обема државама затвором најмање годину дана или тежом казном. Она би се спроводила у складу са постојећим споразумима о екстрадицији које су државе уговорнице међусобно закључиле. Уколико таквог споразума нема, ова конвенција ће се сматрати правним основом за екстрадицију. Држава може одбити да изручи одређено лице (због држављанства или сматра да кривично гоњење траженог лица спада у њену надлежност), али мора не само кривично гонити наведено лице, већ и државу која је замолила за екстрадицију обавестити о крајњем исходу поступка.[31]

Већ смо истакли да ова конвенција прописује да уговорне стране морају да пружају узајамну помоћ у истрагама или поступцима који се односе на кривична дела у вези са рачунарским системима и подацима, и то у најширем могућем обиму. Како би се олакшала и убрзала комуникација, за захтеве за хитну помоћ или обавештења, могу се користити сва средства која имају одговарајуће нивое безбедности и аутентичности попут факса или електронске поште. Уговорне стране су у обавези да поделе и случајне информације

27 D. Agung, *op. cit.*, 52; M. Grotto, *op. cit.*, 5–9; Закон о потврђивању Конвенције о високотехнолошком криминалу.

28 M. Grotto, *op. cit.*, 10.

29 J. Clough, *op. cit.*, 705; Закон о потврђивању Конвенције о високотехнолошком криминалу.

30 M. Vatis, *op. cit.*, 212, 214; M. Keyser, *op. cit.*, 318; Закон о потврђивању Конвенције о високотехнолошком криминалу;

31 M. Vatis, *op. cit.*, 214; Закон о потврђивању Конвенције о високотехнолошком криминалу.

до којих су дошле током својих истрага ако би оне другој страни помогле у њиховим поступцима. Замољена страна може да одбије да пружи помоћ ако захтев сматра политичким деликтом или делом које је повезано са политичким деликтом, ако сматра да то може да јој угрози суверенитет, безбедност, јавни поредак или друге битне интересе, а може и одложити поступање уколико би то угрозило њене кривичне истраге и поступке. Конвенција такође оставља могућност уговорним странама да сву коресподенцију обављају и посредством Интерпола.[32]

У циљу правовремене размене информација, уговорне стране треба да одреде контакт тачку која би била на располагању нон-стоп, тј. 24 сата дневно и 7 дана у недељи како би се обезбедила благовремена помоћ. Те контакт тачке су задужене за олакшавање и директну неопходну помоћ попут саветовања у вези са техничким питањима, чување и прикупљање података, упућивање информација или пак лоцирања осумњичених.[33]

Оно што свакако можемо изнети као недостатак јесте чињеница да ова Конвенција не предвиђа механизме који би осигурали да уговорне стране поштују своје обавезе. Међутим, Европски комитет за проблеме криминала треба да буде информисан о интерпретацији одредби и примени конвенције. Уговорним странама остаје могућност да решавање сукоба решавају путем преговора или било ког по избору мирног решавања спорова. Подношење спора Европском комитету за проблеме криминала је једна од могућности, као и решавање спорова путем преговора, арбитража или уколико се државе договоре, подношењем случаја Међународном суду правде.[34]

4. КРИТИКЕ И НЕДОУМИЦЕ У ВЕЗИ СА ПРИМЕНОМ КОНВЕНЦИЈЕ

Ступање конвенције на снагу је можда у једну руку омогућило међународну сарадњу у области борбе против високотехнолошког криминала, али је довело и до многих дилема, па и критика. Наиме, припадници цивилног друштва указали су да би чвршћа међународна сарадња у овој области могла да угрози приватност и друга људска права. Такође, интернет провајдери су, на пример, били забринути да ће бити доведени у положај да имају више обавеза у погледу пресретања комуникације и чувања података о претплатницима. Такође, Русија, која није уговорна страна, сматра да одељак који се односи на приступ садржају на компјутеру или подацима о корисницима крши национални суверенитет. Остало је отворено питање и шта је са оним сајбер нападима који се не могу подвести под кривична дела, али

32 M. Vatis, *op. cit.*, 215, 220; D. Agung, *op. cit.*, 51, 53; J. Clough, *op. cit.*, 715–716; Закон о потврђивању Конвенције о високотехнолошком криминалу.

33 M. Vatis, *op. cit.*, 215, 217; J. Clough, *op. cit.*, 705–706; M. Keyser, *op. cit.*, 321.

34 M.Vatis, *op. cit.*, 217.

могу представљати другу врсту претње, као што је на пример шпијунажа. Међу критикама налази се и одредба која предвиђа одбијање да се пружи помоћ позивањем на заштиту суверенитета, безбедности, јавног реда и других основних интереса јер државама уговорницама дозвољава превише флексибилности.[35] Постоји још тачки у споразуму које су неодређене и које државама уговорницама остављају широк простор за тумачење. На пример, постоје аутори који у одредби која се односи на обавезу уговорницама да усвоје све правне и друге мере које могу бити неопходне сматрају да постоји неодређеност које су то неопходне мере и да је на државама да процењује. Такође, указује се државе имају могућност да доносе нове кривичне законе, али без упутства или предвиђања како би те измене утпицале на општу популацију корисника интернета. Нарочито се критикује то што не даје стандардни одговор на сајбертероризам.[36] У погледу заштите људских права, критици је изложена и могућа неуједначеност примене, имајући у виду да су неке државе чланице Конвенције о заштити људских права и основних слобода, а неке не. Посебно се указује на то да би овај документ могао да утиче на слободу изражавања и приватности на интернету.[37]

Овај уговор се критикује и због недостатка довољне заштите права држава. Наиме, принципи општег међународног права прописују да ниједна држава не може вршити власт на територији друге државе, нити водити истраге, али ни ухапсити лице на територији друге државе без правног основа, тј. сагласности друге државе да то уради. Могућност једностраног приступа рачунарским подацима на територији друге државе јесте могућност управо прописана овом конвенцијом. Штавише, прекограничне потраге и могућност приступа подацима јесу управо важан аспект модерних криминалистичких истрага.[38] Међутим, држава која је потписала и ратификовала конвенцију без резерве, пристала је на такав вид сарадње, а већ смо говорили о могућим ограничењима у погледу размене информација.

Можемо да се сагласимо са чињеницом да је државама дата слобода да у складу са својим правним системима донесу одговарајуће законе и друге подзаконске акте како би инкриминисале радње у складу са одредбама Конвенције. Можемо да се сагласимо и са сугестијом да се заштита суверенитета, безбедности и јавног реда, а нарочито термин основни интереси могу широко тумачити. Узимајући у обзир да је међународна сарадња у овој области неопходна јер високотехнолошки криминал превазилази државне границе и да је било потребно донети међународни документ који би регулисао ову материју у мери у којој државе са тим желе да се сагласе, одредбе које се односе на могућност државе да одбије сарадњу у конкретном случају можемо тумачити у контексту заштите суверенитета. Када су у питању

35 M. Vatis, *op. cit.*, 218, 220–221.
36 M. Tennis, *op. cit.*, 201–202.
37 *Ibidem*; M. Grotto, *op. cit.*, 5.
38 J. Clough, *op. cit.*, 718.

заштита људских права и страховање да Будимпештанска конвенција може ограничити слободу говора и приватности на интернету, треба имати у виду да је Конвенцијом о високотехнолошком криминалу још у преамбули истакнуто да је потребно спроводити, између осталог, Конвенцију Савета Европе о заштити људских права и основних слобода (1950) и Међународни пакт о грађанским и политичким правима Уједињених нација (1966), који потврђују право сваког појединца на слободно мишљење, слободу изражавања, као и поштовање приватности. Свако има право на слободу мишљења и изражавања. Наведено право подразумева и слободу лица да траже, примају и дају информације и идеје кроз било који медиј и без обзира на границе. Треба само пронаћи баланс између борбе против високотехнолошког криминала и људских права.[39] На државама је свакако да механизме како да спроводе Конвенцију о високотехнолошком криминалу прилагоде заштити основних људских права у складу са Конвенцијом о заштити људских права и основних слобода.

Конвенција је такође критикована, јер не прописује јасан критеријум за решавање спорова,[40] односно оставља широку могућност државама чланицама да одаберу модалитет којим желе да реше међусобне спорове у вези са тумачењем и применом овог уговора. Колико се наведена одредба може тумачити као мањкавост, исто тако то може бити и предност – већа је вероватноћа да ће државе одабрати један од неколико начина да реше спор, него да им се намеће само једно.

Иако ова конвенција прописује могућност екстрадиције, она није загарантована што такође представља предмет критике. Пре свега, екстрадиција може бити одбијена у случају када би то лице било суочено са политичким кривичним делом или уколико би било изложено тортури. Такође, екстрадиција може бити и скупа, тако да је државе чувају само за озбиљна кривична дела. Свакако, екстрадициони аранжмани су између држава inter se, и нико не гарантује да ће екстрадиција бити реализована. То се нарочито односи на земље *common law* система, имајући у виду да оне у складу са својом традициојом не изручују своје држављане, али ту би требало да се примени принцип *aut dedete aut judicare*.[41]

Треба нагласити да поред ограничене територијалне примене, ова конвенција не регулише поступање и сарадњу у свим аспектима сајбер претњи, односно сарадњу у свим областима, него само за кривична дела високотехнолошког криминала прописана конвенцијом, која учине углавном недржавни актери.[42] Очигледно је само аспект високотехнолошких криминала једини сегмент у којој су државе уговорнице желеле да се уговором обавежу.

---

39 Закон о потврђивању Конвенције о високотехнолошком криминалу; H. Koh, „International Law in Cyberspace", *Harvard International Law Journal,* 54/2012, 10.

40 J. Clough, *op. cit.*, 707.

41 *Ibid.*, 717–718; Ж. Новичић, *op. cit.*, 125.

42 S. Shackelford, *op. cit.*, 195.

5. УМЕСТО ЗАКЉУЧКА – КОЈЕ СУ ДРУГЕ ИНИЦИЈАТИВЕ И КОЈА ЈЕ БУДУЋНОСТ КОНВЕНЦИЈЕ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ?

Као што смо могли да видимо у претходним поглављима, високотехнолошки криминал јесте важан безбедносни програм и изазов 21. века. Оно што можемо да очекујемо, јесте даље унапређење међународне сарадње и правила међународног јавног права у овој области. Будимпештанска конвенција о високотехнолошком криминалу зато јесте важан уговор, јер је први документ који инркиминише одређене радње које би против неких лица или друштва били учињени на рачунарском систему. Државе чланице Савета Европе, као и оне које су учествовале у преговорима о овој конвенцији јесу препознале важност сарадње у овој области и пристале су на успостављање међусобног односа по питању борбе против високотехнолошког криминала. У наредним редовима осврнућемо се на друге иницијативе у области информационо-комуникационих технологија. То је важно јер говоримо о материји која није развијена као грана међународног јавног права, а доношење прописа у овој материји није лако изводљиво.

Иако је нама Конвенција о високотехнолошком криминалу најпознатији и најближи, постоје и други уговори који се баве сајбер простором, информационо-комуникационим технологијама и безбедности у области интернета као што су Споразум Шангајске организације за сарадњу у информационој безбедности (2009), али и Конвенција Афричке уније о високотехнолошкој безбедности. На европском континенту, постоје и иницијативе попут иницијативе Организације за европску безбедност и сарадњу кроз „мере за изградњу поверења" у циљу смањења ризика од сајбер сукоба, а наведене мере треба да допринесу размени информација и дијалогу, али и заштити критичке инфраструктуре,[43] дакле, обухвата и превентивне мере.

Било је иницијатива да се сарадња у области безбедности информационо-комуникационих технологија успостави и на глобалном нивоу. Било је чак и иницијатива у оквиру УН и специјализоване агенције Међународне уније за телекомуникације да се донесе свеобухватан споразум за спречавање сајбер рата. Међутим, за тако нешто била је потребна сагласност и воља великих сила које у овом случају није било – САД нису подржале иницијативу. Било је и појединачних иницијатива попут Кине или Русије, међутим и то без успеха. Генерална скупштина УН усвојила је две важне резолуције крајем 2018. године и то „Развој у области информација и телекомуникација у контексту међународне безбедности" (Rez. br. 73/27) и „Унапређење одговорног понашања држава у сајбер простору у конексту међународне безбедности" (Rez. br. 73/266). Постоји и сарадња у оквиру

43 K. Mačak, *op. cit.*, 132.

радних група. На пример, Радна група отвореног типа функционише на нивоу дипломатских представника како би се сагледале могућности за редовни институционални дијалог са учешћем у оквиру УН. Неке друге радне групе су на експертском нивоу.[44] Као што видимо, велике силе још увек не могу да се договоре око модалитета сарадње у овој области.

То што у међународном јавном праву не постоји посебна грана у овој области или свеобухватни документ који регулише односе држава, не значи да сајбер безбедност не подлеже правним правилима. Често се у проналаску адекватних правних правила која би важила у овој области користе већ друге постојеће гране и тамо где је то дозвољено, примењује аналогија. Често се праве поређења са правилима космичког права, нуклеарним оружјем и потенцијалним нуклеарним ратом, правом мора, међународним хуманитарним правом и правилима ратовања.[45] Међутим, са аналогијом треба бити опрезан, сваки од поменутих грана међународног јавног права је специфичан и не може се аналогија у потпуности применити.

Да ли ће и у којој мери доћи до развоја међународног права и сарадње у овој области, зависи највише од држава и њихове жеље да хармонизију правила у овој области, уз уважавање свих специфичности које информационо-комуникационе технологије имају. Једна од основних карактеристика високотехнолошких кривичних дела је то што их учине углавном недржавни актери, а превазилазе државне границе. Такође, постоје и други изазови попут тешкоћа да се идентификује преступник, односно извршилац кривичног дела, затим тешкоће да се сагледају последице наведеног кривичног дела, тешкоће у погледу поступања са електронским подацима који су угрожени, као и проблем да се на брз и ефикасан начин спроведе истрага а да се не наруши поверљивост. С друге стране, државе морају поштовати суверенитет других држава,[46] што је јако тешко имајући у виду прекогранични карактер високотехнолошког криминала. Све су то потешкоће за која треба пронаћи решење да би сарадња држава у овој области била потпуна.

Иако постоје ставови да државе нису биле расположене да понуде јасан *opinio juris* у области информационо-комуникационе безбедности,[47] не можемо рећи да у једном тренутку неће доћи до помака по питању регулисања сарадње у овој сфери. Претходне три године, у оквиру Уједињених нација формиран је *Ad hoc* комитет који је радио на тексту Свеобухватне међународне конвенције о борби против коришћења информационо-комуникационих технологија у криминалне сврхе. Комитет тек треба да изађе са коначним радом и нацртом конвенције.[48] Да ли ће ова конвенција бити

44 Д. Вулетић, *op. cit.*, 318–319; Ж. Новичић, *op. cit.*, 125–126; Вулетић Д., Ђорђевић Б. *et.al.*, *op. cit.*, 241.

45 K. Mačak, *op. cit.*, 131–132; H. Koh, *op. cit.*, 3; S. Shackelford, *op. cit.*, 216–245.

46 Д. Младеновић *et al.*, *op. cit.*, 93; M. Grotto, *op. cit.*, 3; M. Keyzer, *op. cit.*, 310.

47 K. Mačak, *op. cit.*, 130.

48 Више информација о раду Ad hoc комитета на: United Nations, Office for Drugs and Crimes, Ad Hoc Committee to Elaborate a Comprehensive International Convention

прекретница у развоју свеобухватног, универзалног међународног права у овој области, зависиће од самих држава и њихове спремности да прихвате одредбе нацрта документа. То што се преговарало о свеобухватном документу значи да ипак постоји свест о потреби регулисања ове области. Када можемо очекивати конкретне помаке? Када кључне земље покажу интересовање за то – као што је то била кодификација права мора или превенција климатских промена. То ће се догодити када опасност од недостатка регулативе превлада или када је регулатива недовољно развијена. Добар пример и подлога јесу регионалне иницијативе, а до тада остају на снази сви извори меког права управљања интернетом на глобалном нивоу попут резолуција.[49] Остаје да видимо хоће ли Свеобухватна међународна конвенција о борби против коришћења информациони-комуникационих технологија у криминалне сврхе бити та прекретница.

Као што смо у претходним редовима могли да видимо, државама је јако тешко да пронађу консензус на универзалном нивоу и обавежу се уговором на глобалном плану, како због специфичности материје и актера, тако и из политичких разлога. Без обзира на даљи развој међународног јавног права у овој области, Конвенција о високотехнолошком криминалу остаће важан извор када су у питању информационо-комуникационе технологије и сајбер простор. У прилог томе говори чињеница да има преко 70 држава уговорница са свих континената, да су у међувремену потписана још два додатна протокола која у специфичним случајевима интензивирају сарадњу држава у области борбе против високотехнолошког криминала. Без обзира на даље активности на међународном нивоу, остаће камен темељац и у наредном периоду имајући у виду актуелност материје коју регулише, а која се и даље убрзано развија, те стога може послужити и као пример за друге иницијативе.

ЛИТЕРАТУРА

Agung D., „The Role of Interpol in the Settlement of Cybercrime Cases Under the Budapest Convention on Cybercrime", *International Journal of Global Community*, 5, 1/2022, 49–56.

Балтезаревић И., Танчић Д., „Утицај дигиталног окружења на ширење сајбертероризма", *Баштина*, 32, 57/2022, 154–164.

Bunga D., „Legal Response to Cybercrime in Global and National Dimensions", *Padjadjaran Journal*, 6, 1/2019, 69–89.

Clough J, „A world of difference: the Budapest Convention on Cybercrime and the Challenges of Harmonisation", *Monash University Law Review*, 40, 3/2014, 698–736.

on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home, 14. април 2024.

49 Ж. Новичић, *op. cit.*, 126; Д. Младеновић *et.al.*, *op. cit.*, 85–86.

Цветковски С., Кенко В., „Свеобухватни приступ НАТО-а сајбер одбрани“, *Криминалистичке теме*, 19, 5/2019, 501–514.
DeLuca C., „The Need for International Laws of War to Include Cyber Attacks Involving State and Non-state Actors“, *Pace University Scholl of Law*, 3, 9/2013, 278–314.
Grotto M., „Council of Europe Convention on Cybercrime and its ratification in the Italian Legal System“, *Sistema Penal & Violência, Porto Alegre,* 2, 1/2010, 1–17.
Јефтић З. *et al.*, „Савремени конфликти и њихове тенденције“, *Војно дело*, 7/2018, 23–40.
Katagiri N., „Why international law and norms do little in preventing non-state cyber attacks“, *Journal of Cybersecurity*, 2021, 1–9.
Keyser M., „The Council of Europe Convention on Cybercrime“, *J. Transnational Law and Policy*, 12/2003, 287–326.
Koh H., „International Law in Cyberspace“, *Harvard International Law Journal Online,* 54/2012, 1–10.
Mačak K., „Is the International Law of Cyber Security in Crisis?“, *8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2016, 127–139.
Margulies P., „Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility“, *Melbourne Journal of International Law*, 14/2013, 1–24.
Младеновић Д. *et al.*, „Дефинисање сајбер ратовања“, *Војнотехнички гласник*, LX, 2/2012, 84–117.
Младеновић Д., Дракулић М., Јовановић Д., „Неутралност и сајбер ратовање“, *Војно дело*, 63, 3/2011, 189–220.
Новичић Ж., „Нова стратегија сајбер безбедности ЕУ за дигиталну деценију – анализа“, *Развојни правци Европске уније након пандемије COVID 19* (ур. Н. Станковић, Д. Дабић, Г. Бандов), Институт за међународну политику и привреду, Београд, 2021, 123–145.
Радић Н. „Сајбер безбедност и потреба промене модела праћења превара и финансијског криминала“, *Трендови у пословању*, 8, 16/2020, 86–94.
Schmitt M., „“Below the treshold“ cyber operations: the countermeasures response option and International law“, *Virginia Journal of International Law*, 54, 3/2014, 697–732.
Shackelford S., „From Nuclear War to Net War: Analogizing Cyber Attack in International Law“, *Berkeley Journal of International Law*, 27, 1/2008, 191–250.
Tennis M., „A United nations Convention on Cybercrime“, *Capital University Law Review*, 48, 2/2020, 189–235.
Titriga R., „Cyber-attacks and International law of armed conflicts; a „jus ad belum“ perspective“, *Journal of International Commertional Law and Technology*, 8, 3/2013, 179–189.
Vatis M. „The Council of Europe Convention on Cybercrime“, Proceedings of a Workshop on Deterring cyberattacks, Committee on Deterring Cyberattacks:

Informing Strategies and Developing Options; *National Academic Press,* Washington D.C., 2010, 207–223.

Walton B., „Duties Owed: Law-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law", *The Yale Law Journal*, 126, 5/2017, 1460–1519.

Вулетић Д., „Употреба сајбер простора у контексту хибридног ратовања", *Војно дело*, 7/2017, 308–325.

Вулетић Д., Ђорђевић Б., „Проблеми и изазови управљања интернетом на међународном нивоу", *Међународни проблеми*, LXXIII, 2/2021, 235–258.

ИНТЕРНЕТ ИЗВОРИ

Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 189, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189

Council of Europe, Treaty Office, Chart of signatures and ratifications of Treaty 224, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

United Nations, Office for Drugs and Crimes, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

ПРАВНИ ИЗВОРИ

Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичке природе извршених преко рачунарских система, *Службени гласник РС – Међународни уговори*, 19/2009.

Закон о потврђивању Другог додатног протокола уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа, *Службени гласник РС – Међународни уговори*, 7/2022.

Закон о потврђивању Конвенције о високотехнолошком криминалу, *Службени гласник РС – Међународни уговори*, бр. 19/2009.

Katarina Arsić*

CYBER SPACE AND INTERNATIONAL LAW – THE ANALYSIS AND SCOPE OF THE COUNCIL OF EUROPE CONVENTION ON CYBER CRIME

Summary

Cyber space and information-communication technologies are an important topic of the 21st century. Cyber crimes and cyber threats in general are one of the important challenges of today. This paper analyzes the main characteristics of cyberspace. Special emphasis is given to the Convention of the Council of Europe on cyber crime (Budapest Convention) as the first international agreement that prohibits certain actions on computer systems. This convention, which was signed in 2001 and entered into force in 2004, aims to facilitate the harmonization of the laws of the contracting states in the field of combating cyber crime. It's role is to facilitate international cooperation in investigations and criminal matters, also. Analyzing the other initiatives at the regional and global level, we will try to answer the question to which segment of this topic is regulated by international public law, why this document is still current and important, and we will also try to predict in which direction the development of international rules will continue rise to the issue of information and communication technologies.

Keywords: cyber space, cyber crime, information and communication technologies, Budapest Convention, international public law, cyber security.

* PhD student, University of Belgrade, Faculty of Law, katarina.arsic16@gmail.com.