https://doi.org/10.18485/iipe_postkovid.2021.ch6

NOVA STRATEGIJA SAJBER BEZBEDNOSTI EU ZA DIGITALNU DECENIJU – ANALIZA

Žaklina NOVIČIĆ[1]

Apstrakt: Tekst se bavi novom „Strategijom sajber bezbednosti EU za digitalnu deceniju", koju je Evropska komisija krajem 2020. godine predložila a Savet EU usvojio u martu 2021. godine. Taj strateški dokument predstavlja odgovor EU na ubrzanu digitalizaciju i povećano oslanjanje na nove informacione tehnologije – trendove koje je kriza izazvana Kovidom 19 učinila očiglednim. Kroz istorijsko-institucionalni pristup razmotren je najpre međunarodni pravni kontekst nastanka „Strategije", a potom i kontekst prava EU i ograničenja njenih nadležnosti. Materija „Strategije" podeljena je u tekstu na unutrašnji, tehnički i tržišni, i spoljašnji ili vojni aspekt sajber bezbednosti. Analiza dovodi do zaključka da u pogledu spoljašnje sajber bezbednosti EU ima manje nadležnosti, da je strukturno ograničena jednoglasnim odlučivanjem, mada je cela „Strategija" podrobno ažurirana u skladu sa novim trendovima u visokim informacionim tehnologijama.

Ključne reči: sajber bezbednost, digitalizacija, strategija, međunarodno pravo, pravo EU, Zajednička spoljna i bezbednosna politika EU.

Ubrzana digitalizacija i Kovid 19

Trend ubrzane digitalizacije, eksponencijalni rast interneta i sveprisutnost tehnologije postali su očigledni u odgovoru na Kovid 19. Restrikcije kretanja dovele su do enormnog oslanjanja na informacione sisteme, mreže i aplikacije,

[1] Naučni saradnik, Institut za međunarodnu politiku i privredu, Beograd. E-mail: zaklina@diplomacy.bg.ac.rs.

Rad je nastao u okviru naučnoistraživačkog projekta „Srbija i izazovi u međunarodnim odnosima 2021. godine", koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije, a realizuje Institut za međunarodnu politiku i privredu tokom 2021. godine.

a internet saobraćaj povećan je čak za 60% u odnosu na raniji period.[2] Rad na daljinu („od kuće“) praktikovan je gde god je to bilo moguće, a pretpostavlja se da bi on mogao postati i trajniji obrazac.[3] Zavisnost životnih i radnih navika od navedenih trendova učinila je prekide internet saobraćaja, spontane i još više ciljane sajber napade mogućim okidačem lančanih reakcija i paralize većih delova društva i ekonomije. Sajber napadima je u 2020. godini bilo izloženo svako osmo preduzeće, a procena je da su ekonomiji globalno naneli štetu od 5,5 milijardi evra. To su neki od podataka koje navodi Evropska komisija u novoj „Strategiji sajber bezbednosti“, opisujući „najveći transfer ekonomskog bogatstva u istoriji, veći od globalne trgovine drogom“.[4] Bilo kako bilo, Evropska unija je ove godine ažurirala strateški dokument za sajber bezbednost kako bi, kako se navodi, dala dalji doprinos „otpornoj, zelenoj i digitalnoj“ Evropi, odnosno zaštititila „ljude, preduzeća i institucije od sajber pretnji“, ali i „unapredila međunarodnu saradnju“ i osigurala „globalni i otvoreni internet“.[5] „Strategija sajber bezbednosti za digitalnu deceniju“ predstavlja ambicioznu, transformativnu agendu, koja će dalje u tekstu biti podrvrgnuta istorijsko-institucionalnom pregledu i analizi, s prethodnim kratkim osvrtom na međunarodni i evropski pravni kontekst.

Međunarodni pravni kontekst

Jedini obavezujući međunarodni instrument koji se odnosi na sajber bezbednost je „Konvencija o sajber kriminalu“ Saveta Evrope iz 2001. godine (ratifikovana 2004, poznata i kao „Budimpeštanska konvencija“).[6] Do sada ju je

---

[2] Organisation for Economic Cooperation and Development, *Keeping the Internet up and running in times of crisis*, 4 May 2020, Internet: https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/, 10/03/2021.

[3] Društvene posledice opisanih procesa, kada su oni dugotrajni i masovni, ostaju pak pitanje za dublju sociološku elaboraciju.

[4] “The EU’s Cybersecurity Strategy for the Digital Decade”, Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Joint communication to the European Parliament and the Council, Brussels, 16.12.2020, JOIN(2020) 18 final, p. 3.

[5] Ibidem, p. 4, p. 1. Dokumet je usvojen od strane Saveta u martu ove godine: “Draft Council conclusions on the EU’s Cybersecurity Strategy for the Digital Decade”, Council of the European Union Brussels, 9 March 2021, (OR. en) 6722/21.

[6] “Convention on Cybercrime”, ETS No.185, Budapest, 23/11/2001.

potpisalo 66 država, što znači da nema univerzalni karakter.[7] Ona propisuje smernice državama za razvoj nacionalnih zakonskih okvira za borbu protiv sajber kriminala i uspostavljanje okvira za međunarodnu saradnju između država potpisnica. Pod okriljem Organizacija za evropsku bezbednost i saradnju (OEBS) propisane su 2013. godine određene „mere za izgradnju poverenja" radi smanjenja rizika od sajber sukoba, sa fokusom na razmenu informacija i dijalog, zaštitu kritične infrastrukture i promociju javno-privatne saradnje.[8] Međutim, kao ni prethodna ni ova inicijativa nije univerzalna, niti obavezna za sve zemlje članice OEBS ili UN. Pod okriljem Ujedinjenih nacija (UN) sajber bezbednost u kontekstu međunarodne bezbednosti predmet je interesovanja „Grupe vladinih stručnjaka za razvoj u oblasti informacija i telekomunikacija" (*UNGGE*). U izveštaju iz 2013. godine, ova Grupa istakla je stav o primenjivosti i suštinskoj važnosti međunarodnog prava u sajber prostoru.[9] Generalna skupština UN usvojila je krajem 2018. godine dve važne rezolucije o razvoju u ovom kontekstu, od kojih nijedna, interesantno, ne pominje reč „sajber bezbednost": „Razvoj u oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti" (Rez. br. 73/27) i „Unapređenje odgovornog ponašanja država u sajber prostoru u kontekstu međunarodne bezbednosti" (Rez. br. 73/266).[10] Sponzor prve rezolucije bila je Rusija, a protiv nje su glasale SAD i zemlje EU, dok su sponsor druge rezolucije bile SAD, pa su protiv nje glasale brojne zemlje uključujući Rusiju

[7] U Srbiji je usvojena 2009. godine pod nazivom „Konvencija o visokotehnološkom kriminalu" ("Zakon o potvrđivanju Konvencije" objavljen je u Službenom glasniku RS br. 19, od 19. marta 2009), mada u „visoku tehnologiju", pored informacione tehnologije, spadaju i biotehnologija, veštačka inteligencija, nanotehnologija, nuklearna tehnologija, genetski inženjering itd.

[8] "Permanent Council Decision No. 1106 on the initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies", Organization for Security and Co-operation in Europe, 3 December 2013.

[9] Grupa se sastaje periodično od 2004. godine. UN *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Internet: https://digitallibrary.un.org/record/799853?ln=en, 08/07/2021.

[10] "Developments in the field of information and telecommunications in the context of international security", UNGA Res 73/27 (11 December 2018); "Advancing Responsible State Behaviour in Cyber-space in the Context of International Security", UNGA Res. 73/266 (22 December 2018).

i Kinu. Time su, zapravo, pod okriljem UN pokrenuta dva paralelna procesa vezana za sajber bezbednost.[11]

Istaknuti promoter sajber bezbednosti u EU je francuski predsednik Emanuel Makron (*Emmanuel Macron*), koji je sa Foruma za upravljanje internetom 2018. godine pozvao na „poverenje i bezbednost u sajber prostoru".[12] Osim država, u opisani proces uključuju se i drugi „deoničari". Tako je krajem 2019. godine „Globalna komisija za stabilnost sajber prostora" (*GCSC*), sastavljena od više državnih i nedržavnih aktera, objavila preporuke za „unapređenje stabilnosti u sajber prostoru".[13] Velike tehnološke kompanije (*Big Tech*), kao što je Majkrosoft, takođe se uključuju u kampanju za „digitalni mir", upotpunjujući sliku o mnoštvu samozvanih aktera za „popunjavaje postojećih rupa" u multilateralizmu pomoću „multistejkholderizma" (*multistakeholderism*), a da prethodno nisu utvrđene procedure njihove odgovornosti i legitimizacije.[14]

Čini se da „globalno upravljanje internetom" ostaje „siva zona" ispunjena deklaracijama, rezolucijama, izveštajima i mišljenjima, tj. oblast „mekog prava" bez specifičnih „čvrsto" obavezujućih normi univerzalnog karaktera.[15] Ono „čvrsto" međunarodno pravo pak nalazi se, kako smatraju stručnjaci, pred dva glavna izazova u sajber prostoru. S obzirom na jedinstvene karakteristike, tumačenje primene međunarodnog prava na sajber operacije zahteva određeni nivo prilagođavanja. S druge strane, subjekti međunarodnog prava, države

---

[11] Arvind Gupta, "A Tale of two UN Resolutions on Cyber-security," April 24, 2019, https://www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security, 08/06/2021.

[12] V. "Paris Call for Trust and Security in Cyberspace", Internet: https://pariscall.international/en/, 08/06/2021.

[13] *Global Commission on the Stability of Cyberspace*, Internet: https://cyberstability.org/report/, 08/06/2021.

[14] Microsoft, *Digital Peace Now*, 2018, v. Internet: https://digitalpeacenow.org, 08/06/2021. Videti npr.: Jean-Marie Chenou, *Multistakeholderism or Elitism? The Creation of a Transnational Field of Internet Governance*, September 2010, GigaNet: Global Internet Governance Academic Network, ECPR Annual Symposium 2010, Internet: https://ssrn.com/abstract=2809217, 12/03/2019.

[15] Tradicionalno bi se međunarodna standardizacija u oblasti interneta i sajber prostora mogla podvesti pod rad funkcionalnih i strukovnih međunarodnih organizacija poput: Međunarodne organizacije za standardizaciju (ISO), Međunarodne elektrotehničke komisije (IEC) ili Međunarodne telekomunikacione unije (ITU).

prvenstveno, mogu imati različita, ako ne i suprotna tumačenja određenih specifičnih normi međunarodnog prava.[16] Primenjivost međunarodnog prava na sajber operacije ostaje još uvek sporna tema, a i generalno važenje međunarodnog prava u stvarnom svetu takođe je pitanje koje deli (akademsku) javnost. Poslednjih godina više država je pripisivalo sajber napade drugim državama kvalifikujući ih kao nezakonita dela, ali bez preciznog navođenja koje norme su prekršene, ili bez korišćenja međunarodnog pravnog okvira za odgovor na te akte.

Na kraju, međunarodno pravo ostavlja države koje su žrtve sajber operacija bespomoćnim u dva glavna slučaja: u slučaju sajber operacija koje sprovode nedržavni akteri u ime države, jer nove tehnologije nude različite načine za koordinaciju sajber operacija bez visokog nivoa organizacije (problem atribucije, odnosno pitanje kome pripisati sajber napad); pravo odgovornosti država nudi niz rešenja za odgovor na sajber operacije i traženje reparacije, ali ne daje odgovor u svakom slučaju i ne može da reši problem koji se odnosi na tehničke mogućnosti žrtve.[17]

U novoj „Strategiji sajber bezbednosti" EU se poziva na većinu elementa gore opisanog međunarodnog okvira. Ističe se potreba za aktivnijom ulogom u međunarodnoj standardizaciji na ovom području kroz međunarodna i evropska tela za standardizaciju, i najavljuje se usvajanje Strategije standardizacije.[18] Poziva se na „dobrovoljne, neobavezujuće norme, pravila i principe odgovornog ponašanja država", potvrđuje se važnost „Budimpeštanske konvencije" i pozivaju se treće zemlje da joj pristupe.[19] Te „treće zemlje" se okrivljuju za sve veću „fragmentaciju" i „nadmetanje" u ovom kontekstu i upotrebu „međunarodne standardizacije za unapređenje svoje političke i ideološke agende", mada se ne navodi na koje zemlje se tačno misli, što otvara prostor za geopolitičke imaginacije.[20] Ipak, EU sebe vidi

---

[16] François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, pp. 1-2.

[17] Ibidem, p. 496.

[18] Pored pomenutih međunarodnih organizacija i tela za standardizaciju, od evropskih se navode: Evropska komisija za standardizaciju (CEN), Evropski komitet za elektrotehničku standardizaciju (CENELEC), Evropski institut za telekomunikacione standarde (ETSI), Radna grupa za internet inženjering (IETF), Institut inženjera elektrotehnike i elektronike (IEEE) itd. V. "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., p. 20 (n. 101).

[19] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 20-21.

[20] Ibidem, pp. 20-21.

kao lidera u promociji „globalnog i otvorenog interneta“ s fokusom na čoveka, njegovu privatnost, zakonitost, sigurnost i etičnost, što su klasične odlike „meke“ (normativne) moći.[21] Konačno, mada ne najmanje važno, istaknuta je i privrženost pristupu „multistejkholderizma“, koji provejava i celom Strategijom.[22]

Kontekst prava EU

Sliku upotpunjenog normativnog konteksta u kojem je usvojena „Strategija sajber bezbednosti EU“, pruža i osvrt na njen kapacitet za regulaciju u ovoj oblasti prema pravu EU. Pre usvajanja Lisabonskog ugovora,[23] različiti segmenti politike sajber bezbednosti mogli su biti tretirani samo odvojeno, budući da je kapacitet nadležnosti EU bio različit u zavisnosti od toga pod koji „stub“ političkog sistema EU spada odnosno pitanje. Tako su, recimo, krađe velikih količina podataka mogle biti tretirane pod trećim „stubom“ (pravosuđe i unutrašnji poslovi), ali ako bi se radilo o podacima banaka, berzi ili kupaca, to bi moglo imati i značajan uticaj na ekonomsku politiku EU i poverenje na unutrašnjem tržištu (prvi „stub“). Pokušaji da se objedine nadležnosti sa fokusom na kriminal i zaštitu privatnosti građana,[24] ostajali su van Zajedničke spoljne politike i bezbednosti (CFSP), u kojoj se primenjuje jednoglasno usvajanje odluka, uglavnom zbog brige za degradaciju nacionalnog suvereniteta država članica. Zato je pokušaj „strateškog“ pristupa sajber bezbednosti ostajao unutrašnje prirode, u smislu raspodele nadležnosti između nadnacionalnog nivoa EU i država članica, a dokument pod nazivom „Strategija za bezbedno informaciono društvo“ iz 2006. godine nije upućivao na spoljnu sajber bezbednost ili odbranu.[25]

---

[21] Videti odlomak o sajber moći u: Džozef Naj, *Budućnost moći*, Arhipelag, Beograd, 2012, str. 141-184.

[22] “The EU’s Cybersecurity Strategy for the Digital Decade”, op. cit., pp. 21-22.

[23] “Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community”, Official Journal, C 306, 17.12.2007, p. 1-271.

[24] O ranom razvoju na tom polju videti: Žaklina Novičić, „Direktiva o zaštiti podataka u EU“, *Evropsko zakonodavstvo*, Institut za međunarodnu politiku i privredu, Beograd, Br. 11, 2005, str. 9-13.

[25] V. Robert Dewar, “Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy”, Conference Proceedings, EUSA Boston 2015, pp. 10-11, Internet: http://aei.pitt.edu/78992/, 20/03/2021.

Lisabonski ugovor je trebalo da radikalno promeni opisanu situaciju. U njemu se, najpre, izričito spominje krivično delo vezano za računare (*computer crime*, čl. 69b), kao oblast značajna za stabilnost unutrašnjeg tržišta, u kojoj EK može da inicira usvajanje zakona, uz izvršnu moć da osigura da ih države članice sprovode i potencijalnu mogućnost da pokrene postupke za kršenje pravila na području interne sajber bezbednosti. Samo ukidanjem strukture „stubova" trebalo je da omogući razvijanje holističkog i strateškog pristupa spoljnjem aspektu (sajber) bezbednosti, a u tom kontekstu osnovane su i Služba spoljnih poslova (EEAS),[26] kao i Evropska odbrambena agencija (EDA).[27] Direktan rezultat bilo je usvajanje 2013. godine „Strategije sajber bezbednosti EU" pod nazivom „Otvoren, siguran i bezbedan sajber prostor", gde su spojeni razni delovi dotadašnjih „tekovina" EU.[28] Ova strategija po prvi put je spomenula i specifične momente vezane za sajber odbranu pod okriljem Zajedničke spoljne i bezbednosne politike, što je ukazalo na ozbiljnije namere u tom pravcu, ali su nadnacionalne nadležnosti ostale mnogo više ograničene u odnosu na one u pravosuđu i unutrašnjem tržištu. Naime, ključno područje nadležnosti vezano za spoljne sajber pretnje – incidenti sponzorisani od strane drugih država, podvrgnuto je ustaljenim obrascima odlučivanja (jednoglasnost). Sajber bezbednost i spoljna sajber odbrana su, štaviše, po nekim mišljenjima „mikrokosmos mnogo šireg problema nerešenih i nedefinisanih nadležnosti", dok sami Osnivački ugovori EU i dalje izričito priznaju ulogu NATO u pitanjima odbrane i bezbednosti.[29] Mada nova „Strategija sajber bezbednosti EU" detaljnije obrađuje materiju, i dalje ostaju navedena ključna strukturalna ograničenja, što će pokazati dalja analiza.

---

[26] V. Žaklina Novičić, Ivona Lađevac, „Evropska služba spoljnih poslova", *Evropsko zakonodavstvo,* Institut za međunarodnu politiku i privredu, Beograd, 2011, Vol. X, br. 35-36, str. 164-183.

[27] V. Žaklina Novičić, „Novine u spoljnoj i bezbednosnoj politici Evropske unije posle Ugovora iz Lisabona", *Međunarodni problemi,* Institut za međunarodnu politiku i privredu, Beograd, 2011, Vol. LXII, br. 3, str. 404.

[28] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, JOIN/2013/01 final.

[29] Robert Dewar, "Cyber-Lisbon?", op. cit., p. 16.

Unutrašnji, tehnološki i tržišni aspekti nove „Strategije sajber bezbednost EU“

Sudeći po strateškom dokumentu, narednu deceniju EU vidi kao priliku da ostvari vođstvo u razvoju sigurnih tehnologija za čitave lance snabdevanja, industrijske procese, i uopšte „sve stvari povezane sa internetom u EU, bilo da su to automatizovani automobili, industrijski kontrolni sistemi ili kućni uređaji“.[30] Kritična infrastruktura i ključne usluge sve više su međusobno zavisni i digitalizovani, mada se nadalje u „Strategiji“ odvojeno nabrajaju pojedini delovi vezani za ovaj, unutrašnji, više tehnološki i tržišni aspekt bezbednosti, za razliku od onog više povezanog sa spoljnom politikom, bezbednošću i odbranom EU. Dalje, u tekstu osvrnućemo se na svaki taj deo posebno, uz komentare gde je to potrebno.

Mrežni i informacioni sistemi – kritična infrastruktura i usluge

Među pravilima vezanim za digitalno jedinstveno tržište, čiji je deo sajber bezbednost, osnovni pravni instrument je „Direktiva o mrežnim i informacionim sistemima“, čiju reformu je Komisija lansirala istovremeno sa „Strategijom“.[31] Uz to, predložena je i revizija zakonodavstva o kritičnoj infrastrukturi.[32] Kao cilj je proklamovano smanjenje nedoslednosti na unutrašnjem tržištu, poboljšanje izveštavanja o bezbednosti i incidentima, nacionalnog nadzora, kao i kapaciteta nadležnih tela. To bi trebalo da bude osnova za konkretnija pravila čije usvajanje je najavljeno, a koja su neophodna za strateški važne sektore, uključujući energiju, transport i zdravstvo.[33] Komisija je najavila da će do kraja 2022. godine predložiti mere koje uključuju „mrežni kodeks“ (*network code*) sa pravilima za sajber bezbednost u prekograničnim tokovima električne energije. Za finansijski sektor, sličan zakonodavni predlog pokrenut je prošle godine,[34] dok u oblasti

[30] “The EU’s Cybersecurity Strategy for the Digital Decade”, op. cit., pp. 5-13.

[31] “Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148”, COM(2020) 823 final, Brussels, 16.12.2020.

[32] “Proposal for a directive on resilience of critical entities”, COM/2020/829 final, Brussels, 16.12.2020.

[33] “The EU’s Cybersecurity Strategy for the Digital Decade”, op. cit., p. 5.

[34] “Proposal for a regulation on digital operational resilience for the financial sector”, COM/2020/595 final.

avio-saobraćaja već postoje odredbe o sajber bezbednosti, a za druge vrste saobraćaja najavljene su dalje aktivnosti. Kao oblast kritične infrastrukture i usluga, u Strategiji se navodi i budući Svemirski program EU,[35] odnosno jačanje globalnog satelitskog navigacionog sistema nove generacije – *Galileo*. U stvarnosti, glavna infrastruktura ovog sistema nalazi se, zapravo, unutar francuskog vojnog kompleksa.[36]

Interesantno je i zbunjujuće to što su u ovaj skup pitanja, dakle vezanih za kritičnu infrastrukturu, ubrojani i „demokratski procesi i institucije", odnosno jačanje sajber bezbednosti povezano u tom kontekstu. U „Strategiji" se referiše na „Akcioni plan za evropsku demokratiju", dokument čije je usvajanje, u vidu „komunikacije", prošle godine pokrenula EK, smatrajući ga bitnim za zaštitu i unapređenje slobodnih izbora, jačanje demokratskog diskursa i pluralizam medija.[37] Tada je najavljeno, između ostalog, da će EK predložiti i „novi operativni mehanizam za podršku otpornom izbornom procesu", koji će biti organizovan i koordiniran kroz tzv. Evropsku mrežu saradnje u vezi sa izborima, kao podršku angažovanju zajedničkih ekspertskih timova po pitanjima kao što je sajber bezbednost izbora i forenzika na internetu.[38]

Evropski sajber štit

Pod gore navedenim bombastičnim nazivom (eng. *European Cyber Shield*) podrazumeva se, zapravo, mreža operativnih centara za bezbednost (eng. *Security Operations Centres,* „SOC") za prikupljanje i razmenu informacija vezanih za sajber napade i pretnje. Ona bi trebalo da pruža pravovremena upozorenja o mogućim incidentima u sajber prostoru, i da ih stavlja na raspolaganje kako državama tako i drugim zainteresovanim akterima, čime bi

---

[35] V. "European Union Agency for the Space Programme", Internet: https://www.euspa.europa.eu/, 08/06/2021.

[36] V. Amiel Sitruk, Serge Plattard , "ESPI Report 62 – The Governance of Galileo", European Space Policy Institute, January 2017, p. 23.

"What is Galileo?", Internet: https://www.gsc-europa.eu/galileo/what-is-galileo, 08/06/2021.

[37] "Communication on the European Democracy Action Plan", Brussels, 3.12.2020, COM(2020) 790.

[38] "On the European democracy action plan", Brussels, 3.12.2020, COM/2020/790 final.

poslužila kao „pravi štit za sajber bezbednost EU, pružajući čvrstu mrežu stražarskih kula (eng. *watchtowers*), sposobnih za otkrivanje potencijalnih pretnji pre nego što prouzrokuju veliku štetu".[39]

Centralnu ulogu u navedenoj mreži ima Evropska agencija za sajber bezbednosti (*European Union Agency for Cybersecurity, ENISA*), osnovana još 2004. godine, koja analizira potrebe u ovoj oblasti na osnovu kojih bi, prema „Strategiji", EU mogla da se obaveže na preko 300 miliona evra za podršku javno-privatnoj i prekograničnoj saradnji na stvaranju nacionalnih i sektorskih mreža, koje bi uključile i srednja i mala preduzeća. Komisija je predložila da se razviju detaljniji aranžmani upravljanja, operativni principi i finansiranje mreža bezbednosnih operativnih centara, kao i da se podrži obuka i razvoj veština osoblja koje upravlja centrima. Takođe, države članice podstiču se na zajedničko ulaganje u ovaj projekat, s ciljem „stvaranja kolektivnog znanja i razmene najboljih praksi".[40]

U „Strategiji" se ističe da bi bezbednosni operativni centri trebalo da prikupljaju izveštaje na način koji omogućuje organima reda i sudstvu da ih koriste kao dokaze, kao i za izolovanje sumnjivih događaja na mrežama. Otkrivanje aktivnosti zlonamernih datoteka (eng. *malicious executables*) pomaže u suzbijanju sajber napada, što je veoma zahtevan i brz posao, zbog čega bi praktičari trebalo da se pomažu veštačkom inteligencijom (AI), posebno tehnikom mašinskog učenja (*machine learning*), upotpunjenom infrastrukturom super računara (*supercomputer*), koju u EU razvija „Evropsko zajedničko preduzeće za računarstvo visokih performansi", pravni entitet stvoren 2018. godine.[41]

Prilično ambiciozno deluju navedeni zadaci ako se uzme u obzir upozorenje EK sa samog početka Strategije, da trenutno postoji samo ograničena uzajamna operativna pomoć između država članica, da nacionalne vlasti ne prikupljaju i ne dele informacije sistematski, i da prijavljuju samo mali broj incidenata, mada u mnogim od njih već postoje centri za razmenu informacija između javnog i privatnog sektora.[42] Sada se od država članica zahteva da „Grupi za saradnju"

---

[39] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 6-7.

[40] Ibidem, p. 7.

[41] European Commission, *European High-Performance Computing Joint Undertaking*, Internet: https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking, 08/07/2021.

[42] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 3-4.

obezbede i godišnji sumarni izveštaj o pristiglim obaveštenjima o sajber incidentima. S druge strane, ako se ima u vidu broj sajber napada i to da njih najčešće vrše pojedinci, bez potrebe za nekom organizacijom iza njih, postavlja se pitanje zašto bi se sve ovo podizalo na nivo EU, i da li je u tom kontekstu ispoštovan i princip supsidijarnosti.

Ultra bezbedna komunikaciona infrastruktura

Još ambicioznije je zamišljen sledeći aspekt jačanja sajber bezbednosti EU zasnovan na poslednjim dostignućima novih tehnologija, povezujući ih i sa prostorom svemira.[43] Ideja je da se putem kapaciteta za komunikaciju u svemiru osiguraju kritične bezbednosne misije i operacije kojima upravljaju EU i države članice, akteri nacionalne bezbednosti, tela i agencije institucija EU. Važan deo zamišljene ultra bezbedne komunikacione infrastrukture predstavljaju satelitske komunikacije država (*Governmental Satellite Communications, GOVSATCOM*), kao deo budućeg „Svemirskog programa EU". Prostor svemira sve više se vidi kao posebno kritičan za bezbednost, napredak i konkurentnost EU, a satelitska komunikacija kao suštinski element odbrane, bezbednosti, humanitarnog odgovora na vanredne situacije, kao i za diplomatsku komunikaciju. Sve više se računa i na poslednja tehnološka dostignuća vezana za kvantnu komunikacionu infrastrukturu, koja bi državama trebalo da omogući potpuno novi način prenošenja poverljivih informacija pomoću ultra bezbednog oblika šifriranja (enkripcije).

U junu 2019. godine održana je u Bukureštu tzv. Digitalna skupština, kao forum raznih aktera digitalnog jedinstvenog tržišta, i tada je najpre sedam zemalja EU (kasnije se pridružilo još devet) potpisalo „Deklaraciju o saradnji" (*The EuroQCI Declaration*) za razvoj kvantne komunikacione infrastrukture za period 2021–2027. godine.[44] Ovaj projekt bio bi finansiran iz programa Horizont (*Horizon Europe*), Digitalna Evropa (*Digital Europe*), kao i programa „Evropske svemirske agencije" (*European Space Agency*).[45] Deklaracijom su države

[43] Ibidem, pp. 7-8.

[44] V. "The future is quantum: EU countries plan ultra-secure communication network", 8 March 2021, Internet: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network, 15/04/2021.

[45] Deklaraciju o saradnji najpre su potpisale Belgije, Nemačke, Španije, Italije, Luksemburga, Malte i Holandije: Kasnije se pridružilo još devet zemalja: Hrvatska, Kipar, Grčka, Francuska, Litvanija, Slovačka, Slovenija, Švedska i Finska.

potpisnice najavile da će zajedno sa Komisijom raditi na uspostavljanju sigurne kvantne komunikacione infrastrukture za Evropu. Pored svega, Komisija je najavila i da će istražiti moguću primenu multiorbitalnog sistema bezbednog povezivanja, koja bi se nadovezala na postojeće inicijative i koja bi integrisala i druge najsavremenije tehnologije vezane za veštačku inteligenciju (AI), petu generaciju telekomunikacionih mreža (5G), kao i tzv. računarstvo na ivici (*edge computing*).[46]

Nova generacija širokopojasnih mobilnih mreža

Sajber bezbednost povezana sa korišćenjem pete generacije širokopojasnih telekomunikacionih mreža (5G) zauzima poseban odeljak „Strategije". Početkom 2020. godine u dokumentu pod nazivom „Kutija alata za 5G" (*EU 5G Toolbox*) identifikovana je „težnja za najvišim bezbednosnim standardima" u ovoj oblasti.[47] Ova mreža se uzima kao ključna za ekonomski razvoj, kao i za planiranu „zelenu transformaciju". Njen značaj su evropske institucije zabeležile još 2016. godine najavljujući „digitalnu transformaciju" od 2020. godine.[48]

Na poziv Evropskog saveta, Komisija je u martu 2019. godine usvojila „Preporuke o sajber bezbednosti 5G mreža",[49] a u decembru 2020. objavila je Izveštaj o uticaju tih preporuka.[50] Tu je identifikovan „značajan napredak" u ovoj oblasti, kao i to da je većina država članica EU na putu da završi značajan deo implementacije, mada sa određenim varijacijama i preostalim propustima. Na bazi toga, Komisija je pozvala države članice EU da ubrzaju rad na dovršetku sprovođenja glavnih mera iz „Kutije alata" do drugog tromesečja 2021. godine, što bi trebalo da je već obavljeno. U međuvremenu je, u oktobru 2020. godine, i Evropski savet pozvao EU i države članice „da u potpunosti iskoriste 5G alate

[46] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., p. 8.

[47] "Communication on Secure 5G deployment in the EU – Implementing the EU Toolbox", COM(2020) 50, Brussels, 29.1.2020.

[48] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 8-9.

[49] "Recommendation (EU) 2019/534 on the cybersecurity of 5G networks", *Official Journal of the European Union*, L 88, 29.3.2019, pp. 42-47.

[50] "Report on the impacts of the Commission Recommendation of 26 March 2019 on the Cybersecurity of 5G networks", Commission Staff Working Document, Brussels, 16.12.2020, SWD(2020) 357 final.

za internet bezbednost".[51] Akcenat je na koordinaciji radi „smanjenja izloženosti dobavljača visokim rizicima" i „izbegavanju zavisnosti dobavljača na nacionalnom nivou i nivou Unije", zatim na kontinuiranoj razmeni znanja i izgradnji kapaciteta, kao i na osiguranju lanaca snabdevanja itd. Konkretne radnje povezane sa ovim ključnim ciljevima izložene su u posebnom „Dodatku" Strategije.[52]

Jedan od proklamovanih ciljeva „Strategije" jeste „konsolidacija mogućnosti" EU u oblasti mreže 5G, odnosno da se „izbegne zavisnosti" i izgradi „održiv i raznovrstan lanac snabdevanja". Mada to nije eksplicitno navedeno, pretpostavka je da se u kontekstu 5G mreže navedeno odnosi prvenstveno na Kinu.[53]

Dodajmo i to da razvoj novih generacija širokopojasne mreže prate kontroverze vezane za njen zdravstveni uticaj, i da do kraja 2019. godine Komisija nije sprovela nikakvu studiju o potencijalnim zdravstvenim rizicima od 5G tehnologije, što je zabeleženo u izveštaju pripremljenom za Evropski parlament, koji se ovim pitanjem ipak odgovornije pozabavio.[54]

Internet bezbednih inteligentnih uređaja

Internet inteligentnih uređaja ili „Internet stvari" (*Internet of Things*) predstavlja mrežu fizičkih objekata ili „stvari" koje imaju ugrađenu elektroniku, odnosno softver i povezane su na internet na način koji im omogućuje da razmenjuju podatke i bez direktnog učešća čoveka. Te međupovezane sprave već sada premašuju broj ljudi na Planeti, a predviđa se da će ih do 2025. godine biti 25 milijardi, od čega četvrtina u Evropi.[55] Kako se širi „Internet stvari" povećava se i potreba za sajber bezbednošću, što su evropske instucije prepoznale kao još

---

[51] "Special meeting of the European Council (1 and 2 October 2020) – Conclusions", EUCO 13/20, Brussels, 2 October 2020.

[52] V. Appendix, "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 26-28.

[53] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 8-9.

[54] Miroslava Karaboytcheva, "Effects of 5G wireless communication on human health", *EPRS European Parliamentary Research Service*, PE 646.172, March 2020, Internet: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646172/EPRS_BRI(2020)646172_EN.pdf, p. 9, 20/06/2020. Videti i: Samuel Stolton, "MEP: Commission 'irresponsible' on 5G health risks", *Euractiv*, December 12, 2019, Internet: https://www.euractiv.com/section/5g/news/mep-commission-irresponsible-on-5g-health-risks/, 20/12/2020.

[55] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., p. 1 (n. 1).

jednu oblasti svog uticaja.[56] Komisija obećava sveobuhvatan pristup, uključujući moguća nova horizontalna pravila za poboljšanje sajber bezbednost svih „konektovanih proizvoda" i pratećih usluga plasiranih na unutrašnjem tržištu, što je Savet odobrio svojim zaključcima s kraja prošle godine.[57] U Strategiji se nagoveštava da to može stvoriti novi interes evropskih institucija za proizvođače „konektovanih uređaja", za nova softverska i bezbednosna ažuriranja itd. Još neki tehnički momenti napomenuti u „Strategiji" nadovezuju se na predloženu reviziju opštih pravila o bezbednosti proizvoda i ne bave se direktno aspektima sajber bezbednosti, ali prilagođavaju pravila o odgovornosti proizvođača digitalnom kontekstu u okviru regulatornog okvira odgovornosti EU.

Priroda i zastupljenost „Interneta stvari" i mogućnost komunikacije među uređajima bez posredovanja čoveka, mogli bi da predstavljaju potpuno novu paradigmu koja radikalno menja način života u stilu visoke tehnologije. Pitanje je da li danas možemo da domislimo sve eventualnosti u procesima između uređaja koji razmenjuju podatke i odlučuju samostalno i na neuporedivo brži način od čoveka. Da li čak i koncepcija „humanizma" time postaje tesna za opis budućnosti pred nama? Ta pitanja, međutim, otvorila bi „Pandorinu kutiju", a zabrinutost zbog neželjenih ili kontraefekata ovog razvoja, ili elaboracija preterane zavisnosti čoveka od nezavisnih „inteligentnih stvari", ne nalaze mesto u „Strategiji".

Bezbednost globalnog interneta

Srž otvorenog interneta predstavljaju njegovi glavni protokoli i infrastruktura. Oni omogućavaju osnovnu funkcionalnost interneta u celini, odnosno, njegovo normalno funkcionisanje, i smatraju se globalnim javnim dobrom. Tim aspektom sajber bezbednosti bavi se naredni deo Strategije, koji je, ipak, previše opterećen tehničkim detaljima (npr. lokacijama servera itd.), da bismo se ovde šire njime bavili. Uglavnom, EK je najavila da će razviti plan za nepredviđene situacije, podržan sredstvima EU, za rešavanje ekstremnih scenarija koji utiču na integritet i dostupnost sistema u globalnim razmerama. Ono što je brine pak jeste činjenica da se ljudi i organizacije u EU sve više oslanjaju na nekoliko servera kojima

---

[56] Ibidem, pp. 9-10.

[57] "Council Conclusions call for horizontal measures on the cybersecurity of connected devices", 13629/20, Brussels, 2 December 2020.

upravljaju entiteti/kompanije koji nisu iz EU, što ih čini osetljivim na moguće zlonamerne napade, kao i na „velike geopolitičke i tehničke incidente".[58] Od konkretnijih stvari, EK predlaže razvoj regulatornih mera za šestu verziju internet protokola (*IPv4*),[59] zatim diverzifikaciju servera, razvoj javnog evropskog servera, odnosno alternativnog, evropskog servera za pristup globalnom internetu (inicijativa „*DNS4EU*"), koji bi funkcionisao transparentno, u skladu sa najnovijim standardima bezbednosti, zaštite podataka i privatnosti. Sve to trebalo bi da bude deo „Evropskog industrijskog saveza za podatke i oblak" (*European Industrial Alliance for Data and Cloud*). Komisija je najavila da će razmotriti potrebu za stvaranjem mehanizma za sistematičnije praćenje i prikupljanje zbirnih podataka o internet saobraćaju, kao i za savetovanje o potencijalnim poremećajima, što bi mogla biti „Internet posmatračnica" (*Internet Observatory*) unutar aktivnosti „Evropskog centra za industrijsku, tehnološku i istraživačku kompetentnost". Konačno, Komisija je predložila i promociju primene navedenih standarda u partnerskim zemljama (npr. u Africi), kako bi se suprotstavile „zatvorenim modelima interneta zasnovanim na kontroli".

Lanci nabavke tehnologije

Jedan od ciljeva „Strategije" jeste i pojačano prisustvo evropskih firmi u lancima nabavke tehnologije. U budžetu EU za period 2021–2027. godine planirana je pomoć za „bezbednu digitalnu transformaciju", što se označava kao prilika da se pokrene „Nova industrijska strategija za Evropu", odnosno liderstvo u digitalnim tehnologijama i sajber bezbednosti u lancu nabavke koji uključuje podatke i oblak, tehnologiju naredne generacije procesora, ultra bezbedno povezivanje na internet, a prvi put se spominje i naredna generacija mreže 6G. Ovde se direktno referiše na „intervencije javnog sektora", javne nabavke i važne projekte „od zajedničkog evropskog interesa", podršku malim i srednjim preduzećima, a izražena je i nada da će to podstaći privatne investicije, javno-privatno partnerstvo i tzv. rizični kapital (*venture capital*).[60] Cilj je i da se države

[58] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 10-11.

[59] *IPv6* daje mnogo veći prostor za internet adrese (IP), što faktički znači da se „adresa" može dodeliti svakoj stvari koja nekom padne na pamet, i to je pretpostavka daljeg razvoja „Interneta stvari".

[60] Na ovom mestu možda nije zgoreg uputiti na ulog velikih tehnoloških kompanija u lobiranju u Briselu i oko njega, na primer: "Big Tech Lobbying – Google, Amazon & friends and their

članice podstaknu na ulaganje u industriju tehnologija. Predviđa se i podrška za razvoj namenskih programa edukacije za sajber bezbednost, istraživanje i internet inovacije koji razvijaju tehnologije za poboljšanje privatnosti i bezbednu komunikaciju zasnovanu na softveru i hardveru „otvorenog koda". U tom kontekstu, EK podseća na Evropsku mapu za istraživanje i inovacije u oblasti sajber bezbednosti nakon 2020 (*European Cybersecurity Research and Innovation Roadmap*), kao i tzv. čvorišta za digitalne inovacije u programu „Digitalna Evropa" (*Digital Innovation Hubs in the Digital Europe Programme*) itd.[61]

Sve u svemu, u ovom delu Strategije već postaje jasna direktna povezanost koncepcije sajber bezbednosti i budžeta EU. Uglavnom, investicije u sajber bezbednost, posebno kroze „Program za digitalnu Evropu" (*Digital Europe Programme*), „Horizont" i sredstva oporavka od krize izazvane korovavirusom dospeće do 4,5 milijardi u javnim i privatnim investicijama tokom perioda 2021–2027. godine.

Radna snaga sa veštinama vezanim za sajber bezbednost

Poslednji odeljak unutrašnjeg dela „Strategije" odnosi se na radnu snagu, pri čemu se misli na one koji poseduju veštine vezane za sajber bezbednost. Još na početku „Strategije" konstatuje se da postoji veliki nedostatak te vrste radne snage i procenjuje da trenutno 291.000 radnih mesta za takve stručnjake u Evropi nije popunjeno.[62] Sada se najavljuje ulaganje u talente i inovacije „svetske klase", podizanje svesti posebno kod dece i mladih, a svakako ne izostaje ni osvrt na žene koje bi trebalo, prema Strategiji, podstaći da se obrazuju za nauku, tehnologiju, inženjerstvo i matematiku (*STEM*). Komisija je podsetila i na „Revidirani akcioni plan za digitalno obrazovanje" i najavila izradu smernica za podizanje svesti protiv krađa intelektualne svojine koje su omogućene sajber prostorom.[63]

---

hidden influence", *Corporate Europe Observatory*, 23.09.2020, https://corporateeurope.org/en/2020/09/big-tech-lobbying, 08/06/2021.

[61] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., p. 11-12.

[62] Ibidem, p. 3.

[63] Ibidem, p. 12.

Spoljna i vojna dimenzija nove „Strategije sajber bezbednost EU“

Manji deo „Strategije“ bavi se operativnom sposobnošću EU za „sprečavanje, odvraćanje i odgovor“ na sajber napade, kako je u originalnom dokumentu i naznačeno.[64] To, prema ovom dokumetu, podrazumeva: (1) Zajedničku sajber jedinicu; (2) organe vezane za sajber kriminal; (3) sajber diplomatiju; i (4) sajber odbranu. U najkraćem, u odgovoru na pitanje da li ovaj deo nove „Strategije“ daje osnov da se zaključi da je napravljen bitan iskorak u odnosu na prethodni period, mogli bismo reći da je strateški pristup EU sada svakako ažuriran u skladu sa visoko tehnološkim „duhom vremena“, ali da ostaje na snazi ograničavajuća struktura nadležnosti EU vezana uglavnom za jednoglasno odlučivanje u ovim oblastima, kao i ograničenja koja izviru iz globalne raspodele moći i pozicije EU u njoj.

Zajednička sajber jedinica

Kao važan korak ka uspostavljanju evropskog okvira za upravljanje krizama sajber bezbednosti, predstavljena je ideja o „Zajedničkoj sajber jedinici“ (*A Joint Cyber Unit*), koja bi služila kao svojevrsna platforma, i virtuelna i fizička, za saradnju različitih zajednica sajber bezbednosti u EU. Ona bi trebalo da omogući državama članicama, institucijama, telima i agencijama EU, da u potpunosti koriste postojeće strukture, resurse i mogućnosti, sa fokusom na operativnu i tehničku koordinaciju protiv velikih prekograničnih sajber incidenata i pretnji. Preporuke za koordinirani odgovor na sajber incidente i krize velikog obima napisane su još 2017. godine (*Blueprint*),[65] a „Jedinica“ bi obezbedila sredstva da se konsoliduju rezultati u njihovoj implementaciji, posebno u okviru tzv. Grupe za saradnju i tzv. Mreže Ciklon (*CyCLONe*). Konsultacije na jačanju ove arhitekture su počele, u njih je uključen i Visoki predstavnik za spoljnu politiku i bezbednost, a tek se očekuje i „mapiranje“ kapaciteta na nacionalnom i nivou EU, tako da tek ostaje da se vidi šta sve ovo praktično znači.[66]

---

[64] “The EU’s Cybersecurity Strategy for the Digital Decade”, op. cit., pp. 13-19.

[65] “Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises”, C(2017)6100 final, Brussels, 13.9.2017.

[66] “The EU’s Cybersecurity Strategy for the Digital Decade”, op. cit., pp. 13-14.

Sajber kriminal

Tokom prošle godine EU je usvojila dva nova dokumenta u kojima je prepoznata bliska veza između opšte bezbednosne politike EU i sajber kriminala: „Strategija za uniju bezbednosti" i „Agenda protiv terorizma".[67] EK sada najavljuje da će nastaviti „sveobuhvatan pristup" saradnji raznih aktera sajber bezbednosti i održavanja reda ili sprovođenja zakona (kao što je npr. *Europol*), da će dalje organizovati zajedničke konferencije, formulisati izveštaje itd. Predviđeno je i širenje kapaciteta za sprovođenje zakona, uz poštovanje ljudskih prava. U tom kontekstu spominje se posebno i sprečavanje seksualnog zlostavljanja dece *online*, poštovanje opštih forenzičkih standarda, kao i sprovođenje digitalnih istraga, uključujući i kriminal na tzv. *darknetu* (inače, izdvojenim delovima interneta koje standardni pretraživači mreže ne indeksiraju). Budući da su za obavljanje navedenih aktivnosti nužne specifične veštine, *Europol* je određen kao centar ekspertize za podršku nacionalnim vlastima. Komisija je najavila i nastavak rada na obezbeđenju kanala i pojašnjenju pravila za dobijanje prekograničnog pristupa elektronskim dokazima olakšavanjem usvajanja i implementacijom paketa o elektronskim dokazima (*e-evidence package*) i drugih praktičnih mera.[68]

Diplomatska kutija alata za sajber bezbednost

Zajednički diplomatski odgovor na sajber operacije na nivou EU počeo je da se formira 2017. godine. Predlog mera koji je potekao od Komisije, Službe spoljnih poslova (EEAS) i Odbora za politiku i bezbednost (PSC), nazvan je „Kutijom alata za sajber bezbednost" (*Cyber toolbox*) i kasnije je usvojen od strane Saveta.[69] Dalji proces ispunjen je nizom novih sastanaka, izveštaja, zaključaka i komunikacija.[70] U svakom slučaju, sajber prostor je ovim razvojem

[67] "EU Security Union Strategy, COM(2020) 605 final, Brussels, 24.7.2020. "Communication A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond", 9.12.2020, COM(2020) 795 final.

[68] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 15-16.

[69] "Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox)", Council of the European Union, 9916/17, Brussels, 7 June 2017.

[70] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 16-17.

priznat kao razvojni izazov i za spoljnu politiku EU (CFSP), što je u praksi značilo da su tokom prošle godine, u više navrata, sastavljane liste odgovornih za sajber napade – lica i entiteta prvenstveno iz Kine i Rusije.[71] Proces razvoja zajedničkog diplomatskog odgovora na sajber napade podrazumevao bi, zapravo, sposobnost da se brzo pripremi zajednički stav EU (*joint position*). U taj proces su uključeni Visoki predstavnik, infrastruktura Zajedničke spoljne i bezbednosne politike, Radna obaveštajna grupa za sajber bezbednost, Obaveštajni i situacioni centar EU (*EU Intelligence and Situation Centre*, INTCEN), Permanentna strukturirana saradnja (PESCO), kao i ostale postojeće strukture vezane za obaveštajnu aktivnost, suzbijanje dezinformacija, hibridnog stranog uticaja, razvoja situacione svesti i sl. U Strategiji je izražena namera da se pripreme dodatne restriktive mere u oviru „Kutije alata", da se ona integriše u krizni menadžment EU, i da se stvori sinergija sa „Zajedničkim okvirom za suzbijanje hibridnh pretnji" (*Joint Framework on countering hybrid threats*). Ponovo je u ovom kontekstu spomenut i „Akcioni plan za evropsku demokratiju", da bi odmah zatim planirana i pojačana saradnja sa NATO, kao i razmatranje mogućnosti da se kvalifikovanom većinom usvajaju spomenute liste lica i entiteta za sankcije. Bez dalje elaboracije, sugerisana je i mogućnost da se „Kutija alata" sagleda u kontekstu upotrebe ugovornih klauzula o uzajamnoj odbrani i solidarnosti (član 42.7 Ugovora o EU i član 222 Ugovora o funkcionisanju EU). Obe klauzule pokrivaju čitav spektar scenarija koji mogu zahtevati od država članica da obezbede uzajamnu pomoć u slučaju napada, ali odluku o vrsti pomoći ostavljena je državama članicama.[72]

Sajber odbrana

Ambicija za jačanje sajber odbrane EU postavljena je u „Globalnoj strategiji" iz 2016. godine.[73] U planu je da Visoki predstavnik i Komisija predstave novi pregled „Političkog okvira sajber odbrane" (CDPF), kao i da se ojača saradnja

[71] V. Council Decisions (CFSP) 2020/1127; 2020/1537; Council Implementing Regulation (EU) 2020/1125; Council Implementing Regulation (EU) 2020/1536.

[72] Više u: Žaklina Novičić, „Novine u spoljnoj i bezbednosnoj politici Evropske unije posle Ugovora iz Lisabona", op. cit., str. 405-406.

[73] "Council conclusions (14149/16) on implementing the EU Global Strategy in the area of security and defence", Council of the European Union, 14149/16, Brussels, 14 November 2016.

između raznih aktera u pogledu misija i operacija Zajedničke bezbednosne i odbrambene politike (CSDP).[74] Na osnovu toga biće informisan predstojeći „Strateški kompas", kako bi se sajber bezbednost i sajber odbrana dalje ugradile u širu agendu. Politički okvir za sajber bezbednost biće dalje razrađen od strane Vojnog komiteta EU kroz „Vojnu viziju i Strategiju sajber bezbednosti kao domena operacija". Razvoju dalje saradnje doprinela bi i mreža EU-CERT (*EU Military CERT-Network*) koju je formirala EDA, a predviđen je i dalji razvoj kritične infrastrukture u kosmosu od strane Evropske agencije za kosmički prostor i, posebno, centra za bezbednosni monitoring *Galileo*, čiji mandat bi bio proširen i na drugu kritičnu infrastrukturu. Jak naglasak je stavljen na ključne nove tehnologije kao što su veštačka inteligencija, enkripcija, kvantum i sl. Strategijom se ohrabruje razvoj i projekata započetih pod Permanentnom strukturiranom saradnjom (PESCO), a najavljen je i rad i na akcionom planu EK za razvoj sinergije između civilne, odbrambene i svemirske industrije.[75]

Dalja upućenost EU na NATO?

Postavlja se pitanje šta je vredno posebne pažnje u gornjem mnoštvu inicijativa, osim planiranih ogromnih budžetskih izdvajanja. Po našem mišljenju, važno je podsetiti još jednom da su spoljna politika, bezbednost i odbrana i dalje oblasti jednoglasnog odlučivanja, što praktično znači pravo veta država članica EU. Znaju to dobro i u EU, pa tako nemačka diplomatija baš ovih dana obnavlja kampanju da se to kvalifikovanom većinom zameni pravilo jednoglasnog odlučivanja.[76] Dok se to ne desi, ako se i desi – budući da bi to, ujedno, bio i odlučujući korak ka federalnoj EU, što je u ovom momentu ipak malo verovatno, EU je i dalje ograničena na projektovanje svog posebnog, normativnog imidža, građenog prvenstveno na zaštiti osnovnih ljudskih prava, ukratko – na projekciji tzv. meke moći.

---

[74] Žaklina Novičić, „Evropska unija u krizi: politika bezbednosti i odbrane", u Aleksandar Gajić, Milan Igrutinović (urs), *Kriza Evropske unije*, Institut za evropske studije, Beograd, 2013, str. 157-184.

[75] "The EU's Cybersecurity Strategy for the Digital Decade", op. cit., pp. 18-19.

[76] "Germany calls for abolition of 'paralysing' EU member states foreign policy veto", *Euronews*, 08/06/2021, Internet: https://www.euronews.com/2021/06/08/germany-calls-for-abolition-of-paralysing-eu-member-states-foreign-policy-veto, 12/06/2021.

Standardi privatnosti, zaštite podataka ili zaštite dece *online*, čini nam se da su ono vrednije u digitalnoj/sajber politici EU, barem u poređenju sa ostalim delovima sveta. U tom kontekstu važno bi i neophodno bilo da se, pre svega, ustanovi jasna i nedvosmislena definicija pojma „sajber bezbednost", što važi i za svrhe daljeg razvoja „Strategije".[77]

Nedostatak jasno definisane nadležnosti EU u pitanjima odbrane i bezbednosti, kao i usmerenost na NATO u vojnim stvarima, upućuju na potrebu da se istakne da je ovaj vojni savez već proglasio sajber napade zonom svoje odgovornosti, što je sumirano u nedavnoj izjavi generalnog sekretara Jensa Stoltenberga, da u odgovoru na takvu vrstu „agresivnog ponašanja" može biti aktiviran i član 5 osnivačkog ugovara NATO.[78] Šta bi to konkretno značilo u sajber prostoru – može biti predmet rasprave. Na ovom mestu podsetićemo na načelni stav nemačkog Saveznog ustavnog suda, prema kojem obaveza iz navedenog člana „ne podrazumeva nužno upotrebu vojnih sredstava, već državama članicama NATO daje određeni prostor za procenu u pogledu sadržaja pomoći koja će biti pružena".[79] Drugim rečima, obaveza vojne pomoći iz člana 5 Ugovora o NATO, i nezavisno od nove vrste (sajber) napada, pre je političke nego pravne prirode. Koliko to, međutim, nije utešna misao, i koliko politička obaveza može da nadjača svako pravno razmatranje, poznato je, recimo, iz primera agresije NATO na SR Jugoslaviju 1999. godine (mimo odluke Saveta bezbednosti UN i većine nacionalnih parlamenata država članica). To jasno upućuje na zaključak da bi i pri odlučivanju o eventualnoj primeni člana 5 u odgovoru na sajber napad prevagu imala arbitrarnost, kontekstualnost i geopolitika. U ovom slučaju, čini se da pozivanje na čuveni Član 5 ima pre za cilj zastrašivanje, eventualno odvraćanje i demonstraciju snage, nego što bi trenutno mogla da se zamisli njegova konkretna upotreba.

---

[77] Videti mišljenje o „Strategiji sajber bezbednosti EU" evropskog supervizora za zaštitu podataka: Wojciech Rafał Wiewiórowski, "Summary of the Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive", *Official Journal of the European Union*, C 183/3, Brussels, 11 March 2021.

[78] John Grady, NATO's Stoltenberg: Sophisticated Cyber Attacks Could Trigger Collective Response, June 8, 2021, https://news.usni.org/2021/06/08/natos-stoltenberg-sophisticated-cyber-attacks-could-trigger-collective-response

[79] "Urteil des Zweiten Senats vom 30. Juni 2009", BVerfG, 2 BvE 2/08, para. 386.

Na kraju, još uvek „siva zona“ politike – sajber bezbednost, predstavlja polje institucionalno složenih odgovornosti i aktivnosti, i kao takva, može da bude pogodna za razne manipulacija, što ne treba gubiti iz vida i analize. To je posebno važno kada se sumnja na umešanost država u sajber napade, odnosno kada se javi teškoća da se precizno locira i identifikuje počinilac napada (problem atribucije). To je ozbiljno ograničenje ne samo za EU i NATO, već i za razvoj međunarodnog prava prilagođenog sajber prostoru u kontekstu međunarodne bezbednosti.

U svakom slučaju, dalji razvoj visoke informacione tehnologije, eksponencijalni rast „Interneta stvari“, širokopojasnih mreža novih generacija, kvantnog računarstva i ostalih inovacija sa za sada nepojmljivim pravcima implikacija, otvara za ceo svet neistraženu i nesigurnu perspektivu. Ne sme biti zanemarena etička dimenzija takvog razvoja, kao ni potreba demokratske elaboracije. Ubrzanoj digitalizaciji morale bi da prethode otvorene javne rasprave, kako u zemljama članicama EU tako i u onima koje se tome prilagođavaju, ili kopiraju razvoj u EU i svetu.

Literatura

Chenou, Jean-Marie, *Multistakeholderism or Elitism? The Creation of a Transnational Field of Internet Governance*, September 2010, GigaNet: Global Internet Governance Academic Network, ECPR Annual Symposium 2010.

Delerue, François, *Cyber Operations and International Law*, Cambridge University Press, 2020.

Dewar, Robert, “Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy”, Conference Proceedings, EUSA Boston 2015.

Karaboytcheva, Miroslav, “Effects of 5G wireless communication on human health”, *EPRS European Parliamentary Research Service*, PE 646.172, March 2020.

Naj, Džozef, *Budućnost moći*, Arhipelag, Beograd, 2012.

Novičić, Žaklina, „Direktiva o zaštiti podataka u EU“, *Evropsko zakonodavstvo*, Institut za međunarodnu politiku i privredu, Beograd, Br. 11, 2005, str. 9-13.

Novičić, Žaklina, „Evropska unija u krizi: politika bezbednosti i odbrane“, u Aleksandar Gajić, Milan Igrutinović (urs), *Kriza Evropske unije*, Institut za evropske studije, Beograd, 2013, str. str. 157-184.

Novičić, Žaklina, Ivona Lađevac, „Evropska služba spoljnih poslova“, *Evropsko zakonodavstvo,* Institut za međunarodnu politiku i privredu, Beograd, 2011, Vol. X, br. 35-36, str. 164-183.

Novičić, Žaklina, „Novine u spoljnoj i bezbednosnoj politici Evropske unije posle Ugovora iz Lisabona“, *Međunarodni problemi,* Institut za međunarodnu politiku i privredu, Beograd, 2011, Vol. LXII, br. 3, str. 397-417.

Sitruk, Amiel and Serge Plattard , “ESPI Report 62 – The Governance of Galileo”, European Space Policy Institute, January 2017.

Wiewiórowski, Wojciech Rafał, “Summary of the Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy and the NIS 2.0 Directive”, *Official Journal of the European Union*, C 183/3, Brussels, 11 March 2021.

NEW EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE – AN ANALYSIS

Abstract: The text deals with the new EU'S Cybersecurity Strategy for the Digital Decade proposed by the European Commission at the end of 2020 and adopted by the Council in March 2021. This strategic document represents the EU's response to accelerated digitalisation and increased reliance on new information technologies - the trends made apparent by the COVID-19 crisis. First of all, the international legal context of the “Strategy” is considered, and then the context of EU law and the limitations of its competencies. The subject matter of the “Strategy” is divided into internal, technical, and market dimensions and, on the other hand, external or military aspects of cyber security. The analysis led to the conclusion that the EU has fewer competences in terms of external cyber security and that it was structurally limited by unanimous decision-making. Nevertheless, the entire “Strategy” has been updated in detail in line with new high information technology trends.

Keywords: the EU, Cybersecurity Strategy, digitalization, international law, EU law, Common Foreign and Security Policy (CFSP).