NOVA STRATEGIJA EU ZA KIBERNETSKU SIGURNOST U DIGITALNOJ DECENIJI EU

Mr. Tijana Bombol Delevska

Pregledni članak

Sažetak: Nova strategija EU za kibernetsku sigurnost uvodi nova pravila za povećanje otpornosti ključnih fizičkih i digitalnih entiteta. Strategija je usmjerena na izgradnju digitalne budućnosti Europe, sigurnosne unije sa snažnim utjecajem na zemlje na putu ka EU. Ključno pitanje je kako ojačati evropsku kolektivnu otpornost na cyber prijetnje, kao i omogućiti svim građanima i preduzećima da u potpunosti iskoriste ove usluge i digitalne alate? Republika Sjeverna Makedonija izražava spremnost da ojača svoje kapacitete za borbu protiv ovih prijetnji. U tu svrhu ostvaruje uspješnu saradnju sa zemljama u regionu, posebno u pogledu razmjene informacija i iskustava za smanjenje sajber prijetnji. Glavni cilj ove strategije je jačanje međunarodnih normi i standarda u cyber prostoru, koji je osnova za vladavinu zakona, poštovanje ljudskih prava i sloboda i integritet institucija. Ova strategija iz decembra 2020. godine želi zaštititi globalni i otvoreni Internet i primijeniti zaštitne mjere koje garantiraju sigurnost uopće. Strategija sadrži konkretne prijedloge za regulatornu, investicijsku i političku inicijativu u tri područja djelovanja EU: otvorenost, tehnološki suverenitet i vođstvo; izgradnja operativnih kapaciteta za prevenciju, odvraćanje i reagovanje i promociju globalnog i otvorenog cyber prostora uz povećanu saradnju. Bit će od velike važnosti proučiti strukturu ove strategije i njen utjecaj na nacionalni model kibernetičke sigurnosti u Republici Sjevernoj Makedoniji.
Ključne riječi: sigurnost, zaštita, slobode i prava, vladavina zakona, cyber prostor.

THE NEW EU CYBERSECURITY STRATEGY IN THE EU DIGITAL DECADE

Abstract: The new EU cybersecurity strategy introduces new rules to increase the resilience of key physical and digital entities. The strategy is aimed at building the digital future of Europe, a security union with a strong influence on the countries on the road to the EU. A key question is how to strengthen Europe’s collective resilience to cyber threats, as well as enable all citizens and businesses to take full advantage of these services and digital tools? The Republic of North Macedonia expresses it`s readiness to strengthen its capacities to fight against these threats. For that purpose, it realizes successful cooperation with the countries in the region, especially in terms of exchange of information and experiences for reduction of cyber threats. The main goal of this strategy is to strengthen international norms and standards in cyberspace, which is the basis for the rule of law, respect for human rights and freedoms and the integrity of institutions. This strategy from December 2020 seeks to protect the global and open Internet and to implement safeguards that guarantee security in general. The strategy contains concrete proposals for regulatory, investment and policy initiative in the three areas of EU action: openness, technological sovereignty and leadership; building operational capacities for prevention, deterrence and response and promotion of global and open cyberspace with increased cooperation. It will be of great importance to study the structure of this strategy and its impact on the national model of cyber security in the Republic of Northern Macedonia.
Keywords: security, protection, freedoms and rights, rule of law, cyberspace.

Uvod

Prevencija i represija zločina, bilo da se radi o globalnom, regionalnom ili nacionalnom fenomenološkom obliku, temelji se na određenoj strategiji. Stoga razlikujemo nacionalne, regionalne i globalne strategije za pravovremeni odgovor na cyber prijetnje koje stvarno postoje i uzrokuju štetne posljedice. Pored toga, različite vrste strategija razlikuju se u zavisnosti od oblika kriminala koji se pojavljuje. U njemu se navodi da "strategija djelovanja u određenom području znači najefikasniju taktiku djelovanja (aktiviranjem najoptimalnijih načina i metoda) koja se realizuje u okviru opće platforme ili koncepta za buduću provjeru globalnih postavki ili za realizaciju i rješavanje temeljna pitanja i konkretni projektirani zadaci u strogo određenom polju nauke ili u određenom praktičnom društvenom životu Projekcija i realizacija postavljenih osnovnih pitanja i strogo definisanih zadataka, čija je namena sprovođenje u budućem konkretnom datom, uglavnom, dugoročnijem periodu, zapravo odražavaju i strateške ciljeve koje bi u okviru odgovarajuće globalne koncepcije određenog društvenog područja trebali provoditi nositelji takve platforme.[258] Strateški pristup trebao bi pokazati način za postizanje unaprijed definiranih ciljeva koji imaju širi društveni, ali i globalni značaj. Tako na primer, "strategija policijske organizacije definira se kao skup jasno definiranih ciljeva, popis glavnih zadataka i izbor odgovarajućih aktivnosti uz predviđanje i alokaciju resursa nepophodnih za funkcioniranje organizacije kako bi se postigli postavljeni ciljevi. Postoje tri nivoa ciljeva:

(1) strategisjki, kojim se formulira strategija policijske organizacije;

(2) taktićki, kojim se definira taktika za postizanje pojedinih strategijskih siljeva i

(3) operativni, vezan za neposredno provođenje zadataka. "[259]

Svaka zemlja nastoji postaviti temelje nacionalne strategije u borbi protiv kriminala. Treba naglasiti da strategija nije deklarativni pamflet, već dokument od globalnog značaja u postavljanju sigurnosne arhitekture. Naime, svakodnevne radnje ovlaštenih službenika u otkrivanju, razjašnjavanju, dokazivanju i sprečavanju zločina nezamislive su bez prethodnog postavljanja strateškog okvira koji bi trebao biti izraz jasno postavljenog cilja nulte tolerancije za zločin. U tom pravcu je postavljeno mišljenje da "strateški pristup u djelovanju države vlasti, policija (čak i kriminalistička policija) i drugih društvenih subjekata, samo je jedan od novih zahtjeva i izazova koji se nameću da budu zreli za ono što nam se sada događa na polju kriminala ili će nam se dogoditi u bliskoj budućnosti." Svijet već dugo uči o proaktivnom, strateškom, koordiniranom pristupu radu policije i drugih dijelova društva."[260] "Pritome,

[258] Ангелески М., Криминалистички теории, Скопје, 2014 година, стр. 147.
[259] Modly D., ŠuperinaM., Korajlič N., Rječnik kriminalistike, Strukovna udruga kriminalista, Zagreb, 2008 godina, str. 785.
[260] Simonović B., Strateški pristup kriminalističke policije u kontroli kriminala – međunarodni propisi, pojmovno određenje, neki izazovi implementacije, Zbornik radova: Kriminalističko forenzička istraživanja, Vol. 4, br. 1, Banja Luka, 2011 godina, str. 28.

značajne tendencije u savremenom pristupu preventivno-represivnoj borbi protiv kriminaliteta jesu:

1.jačanje proaktivnog pristupa, nasuprot tradicionalno reaktivno delovanje;

2.strateško planiranje kriminalističke djelatnosti;

3.intenzivna saranja među državama u borbi protiv kriminaliteta;oge forenzičkih istraživanja i metoda, s posebnim osvrtom na kriminalističko-forenzičke analitičke zadatke;

4.kriminalistički inteliđens."[261]

4.povećavanje u

Naša zemlja gradi vlastitu strategiju u borbi protiv cyber kriminala i zasniva se na nacionalnim strateškim prioritetima, uključujući dužno poštovanje evropskih propisa u ovoj oblasti.

1. Temeljna osnova Strategije EU za kibernetsku sigurnost 2020

Od svog osnivanja, Europska unija uspostavlja ozbiljnu osnovu za rješavanje cyber prijetnji i njihovih izazova. Stoga, pored ostalih tijela, Vijeće Evrope, usvajanjem važnih preporuka, doprinosi državama članicama da primijene nove algoritme i modele u praktičnoj borbi protiv ovog zločina. Time se ovaj cilj postiže strateškom saradnjom država, odnosno razmjenom informacija i drugim oblicima komunikacije između država koje u tu svrhu potpisuju memorandume o saradnji.

Potkraj 2020. godine Komisija i visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku pokrenuli su novu strategiju EU o kibernetičkoj sigurnosti. Glavni cilj usvajanja ovog dokumenta je "postići zaštitu globalnog i otvorenog Interneta, ali u isto vrijeme ponuditi zaštitne mjere koje garantiraju sigurnost, ali i zaštitu evropskih vrijednosti i temeljnih prava svih građana. Kao ključni dio Izgradnje evropske digitalne budućnosti, evropskog plana oporavka i strategije sigurnosne unije EU, ova strategija će ojačati kolektivnu otpornost Europe na cyber prijetnje i omogućiti svim građanima i preduzećima da u potpunosti koriste pouzdane i sigurne usluge nova strategija kibernetičke sigurnosti omogućava Uniji da učvrsti svoje vodstvo na polju međunarodnih normi i standarda u cyber prostoru i ojača suradnju s partnerima širom svijeta u cilju promicanja globalnog, otvorenog, stabilnog i sigurnog cyber prostora koji je zasnovan na vladavini zakona, ljudskim pravima, temeljnim slobodama i demokratskim vrijednostima."[262]

Ova se strategija temelji na temeljnim temeljnim civilizacijskim vrijednostima vezanim za temelje na kojima je stvorena Europska unija. Za evropske vrijednosti i principe, sigurnost nije samo osnovni preduvjet lične sigurnosti, već štiti i temeljna prava i temelj je povjerenja ...

[261] Kozarev A., Savremeni pristup u borbi protiv organizovanog kriminaliteta u RM, Zbronik radova - VI Naučni skup: Dani bezbjednosti, Univerzitet Sinergija, Banja Luka, 2012 godina, str. 348.

[262] https://ec.europa.eu/croatia/News/new_eu_cybersecurity_strategy_and_new_rules_to_make_physical_and_digital_critical_entities_more_resilient_hr, 17.03.2021.

Europljani se danas suočavaju s nestabilnim sigurnosnim okruženjem pod utjecajem novih prijetnji i drugih čimbenika, uključujući klimatske promjene ., demografski pokreti i politička nestabilnost. Cyber napadi i cyber kriminal i dalje rastu. "Sigurnosne prijetnje postaju sve složenije: izloženi su mogućnosti prekograničnog kriminala i međuovisnosti, zloupotrebljavaju nestajanje granica između fizičkog i digitalnog svijeta i iskorištavaju ranjive skupine, kao i socijalne i ekonomske razlike."[263]

2. Struktura EU strategije kibernetičke sigurnosti 2020

Nova strategija EU za kibernetsku sigurnost od 2020. ima za cilj osigurati cyber i fizičku otpornost ključnih entiteta i mreža. Pored ove strategije, Evropska komisija nudi prijedloge za rješavanje ovih pitanja sa:

- Direktiva o mjerama za visoku zajedničku razinu kibersigurnost u cijeloj Uniji (revidirana Direktiva NIS ili NIS 2) i
- Nova Direktiva o otpornost ključnih subjekata.

Te a oi a obuhvaćaju brojne sektore, a cilj im je usklađeno i komplementarno rješavanje postojećih i budućih rizika na internet i izvan njega, od kibernapada do kriminala ili prirodnih katastrofa.

Po svom sadržaju, ova strategija uključuje konkretne prijedloge regulatornih, investicijskih i političkih inicijativa u tri područja djelovanja EU, naime:

1.Otpornost, tehnološka suverenost i vodstvo

U okviru tog područja Komisija predlaže reform pravila o sigurnosti mrežnj i informacijskih sustava na temelju Direktive o mjerama za visoku zajedničku razinu kibersigurnosti u cijeloj Uniji, ako bi se povećala razina kiberotpornosti klučnih javnih i privatnih sektora: bolnice, energetske mreže, željeznice, ali i podatkovni centri, javne uprave, istraživački laboratoriji i proizvodnja ključnih mediciskih proizvoda i lijekova te ostala ključna infrastruktura i usluge moraju ostati nepropusni u prijetećem okruženju koje se sve brže mijenja i sve je složenije.

2.Izgradnja operativnih kapaciteta za sprečavanje, odvraćnje i odgovor

U ovom sadržaju važan je pijedestal za uspostavu novu zajedničku jedinicu za kiersigurnsot radi jačanja suradnje između tijela EU-a i tijela država članica odgovornih za sprečavanje kibernapada, uključujući civilne, diplomatske i kiberobrambene zajaednice itd. Cilj je poboljšati saradnju u ovom području razvijanjem najsavremenijih sigurnosnih dizajna, uz uključivanje Evropske odbrambene agencije i pomoći iz Europskog fonda za odbranu.

3.Unapređivanje globalnog i otvorenog kiberprostora povećanom suradnjom

[263] Europska komisija, Komunikacija komisije Europskom parlamentu, Europskom Vijeću, Vijeću, europskm gospodarskom i socijalnom odboru te odboru regija, o strategiji EU-a za sigurnosnu uniju, Bruxelles, 24.07.2020, str. 2.

Ovaj sadržaj usredotočen je na postizanje temeljnih ciljeva globalnog poretka koji je u velikoj mjeri određen međunarodnom sigurnošću i stabilnošću. Pitanje je poštivanja evropskih vrijednosti izraženih kroz međunarodne norme i standarde. Od velike je važnosti prijedlog Unije za jačanje cyber dijaloga s trećim zemljama, regionalnim i međunarodnim organizacijama kako bi se uspostavila mreža EU za cyber diplomatiju. Program Digitalna Evropa je od suštinske važnosti, kao i evropski plan oporavka.Cilj je ostvariti zajednička ulaganja EU-a, država članica i tog industrijskog sektora u iznosu od 4,5 milijardi eura, prije svega u okviru Centra za stručnost u području kibersigurnosti i Mreže koordinacijskih centara.

3. Impakt primjene strategije EU za kibernetsku sigurnost od 2020

Europska unija, usvajanjem Strategije sigurnosti, strategije kibernetičke sigurnosti, ali i mnogih drugih dokumenata, a s njima u vezi institucionalnog djelovanja niza evropskih tijela i tijela, izražava ozbiljnu namjeru da se pozabavi izazovima vezanim za cyber sigurnost. Postoji nekoliko razloga za to:

- Kiberprijetnje se nastavljaju razvijat s obzirom na sve veću digitalizaciju i međusobni povezanost
- Prevladanje lažna dihotomija između događaja na internet i izvan njega
- Zaštita ključnih usluga i infrastrukture od cyber napada i fizičkih rizika i više.

Pored utjecaja ove strategije na propise u državama članicama, od velikog je značaja i njeno proučavanje i praćenje od strane zemalja kandidata za članstvo u Uniji. Naša zemlja ulaže ogromne kapacitete u ovo područje. Europska perspektiva je vrvni prioritet. "S jedne strane, pre svega u deklarativnom smislu, postoji jasno izražena politička volja kod političkih lidera i njihovih partija za što vrži ulazak naše države u EU. Takva fokusiranost koja se provlači kroz vrhunske nacionalne dokumente postoiji i koj ključnih institucija u sistemu bicefalne organizacije vlasti u državi: Parlament, Vlada, predsednik Republike. "[264]

Time je usvojena Nacionalna strategija za cyber sigurnost Republike Sjeverne Makedonije[265] - strateški a oi a koji bi trebao služiti kao putokaz za razvoj sigurnog, sigurnog, pouzdanog i izdržljivog digitalnog okruženja, podržanog kvalitetnim kapacitetima, koji se temelje na povjerenju i saradnji na polju kibernetičke sigurnosti. Ova strategija razvijena je u skladu sa Strategijom kibernetske sigurnosti Evropske unije i NATO-ovom politikom kibernetske sigurnosti i opredjeljenošću za pružanje sigurnog, sigurnog, pouzdanog i otpornog digitalnog okruženja u korist građana, preduzeća i javne uprave. Strategija je povezana sa:

- Aktivnosti, socijalne interakcije, ekonomija, a oi osnovna ljudska prava i slobode usko su povezane sa primjenom IKT, zbog čega je neophodno osigurati otvoren, siguran i siguran cyber a oi a;

[264] Kozarev A., Uloga Sekretarijata za evropska pitanja Vlade RM u savlađivanju savremenih izazova procesu integracije u EU, Zbornik radova: Evropska unija i Zapadni Balkan - izazovi i perspektive, Institut za međunarodnu politiku i privredu i Hans Seidel Stiftung, Beograd, 2014 godina, str. 417.
[265] http://morm.gov.mk/wp-content/uploads/2018/07/ns_sajber_bezbednost_2018-2022.pdf, 18.03.2021 god.

- Korištenje ICT a oi a i razvoj elektroničkih usluga povećava rizik od cyber incidenata i zloupotreba, što ove prijetnje čini jednom od najozbiljnijih po nacionalnu sigurnost;
- Definisanje i razvoj politike cyber odbrane;
- Uspostaviti integrirani, multidisciplinarni pristup kako bi se osigurala bliža saradnja i koordinacija između sektora odbrane i bezbjednosti, institucija uključenih u borbu protiv kibernetičkog kriminala, privatnog sektora, građana i organizacija civilnog društva i drugih relevantnih dionika.;
- Jačanje operativnih kapaciteta, koordinacije i saradnje između relevantnih institucija i organizacija uključenih u borbu protiv cyber kriminala;
- Uspostavljanje zajedničkih standarda, obuka i obrazovanje svih institucija i organizacija uključenih u razvoj sajber sigurnosti;
- Jačanje institucionalnog i pravnog okvira na polju sajber sigurnosti.
- Jačanje nacionalnih kapaciteta za prevenciju i zaštitu od cyber napada, a oi provođenje aktivnosti za podizanje nacionalne svijesti o cyber sigurnosti.

Utjecaj Evropske strategije kibernetske sigurnosti 2020 određen je Direktivom na zabrinutost zbog visoke zajedničke cyber sigurnosti u Uniji (revidirana Direktiva NIS ili NIS 2), kao i na uspješno djelovanje Evropske agencije za kibernetsku sigurnost (ENISA). EU za 5G i buduće generacije mreža.

S obzirom na ove činjenice, može se primijetiti da će utjecaj kibernetske strategije EU od 2020. godine omogućiti:

1. jačanje industrijskih i tehnoloških kapaciteta Unije na polju cyber sigurnosti;

2. udruživanje evropskih resursa za postizanje ciljeva strategije;

3. pružanje vodeće uloge u postizanju cyber sigurnosti;

4. povećati razmjenu informacija i saradnju u slučajevima cyber krize na nacionalnom nivou ili na nivou EU;

5. pružanje efikasne zaštite evropske kritične infrastrukture i više.

Zaključak

Digitalna transformacija u Europi je stvarnost i zato ulaganja u nju ubrzano rastu iz godine u godinu. Ali ovom digitalnom ekspanzijom raste i svijest građana o potrebi veće sigurnosti. Također, međunarodnu sigurnost sve više određuje cyber sigurnost, jer cyber prijetnje svakodnevno mijenjaju svoju etiologiju i fenomenologiju. U tako surovoj stvarnosti, usvajanje cyber strategije 2020. godine od strane EU više je nego potrebno. Istovremeno, proces njegove primjene omogućit će vladama, kao i građanima, organizacijama da povećaju svoje napore u zaštiti od globalnih cyber prijetnji. Stoga se može reći da je ova strategija važan regulator algoritama, modela i predloženih rješenja za zaštitu od cyber napada. Stoga se može reći da kroz ovu strategiju, ali i mnoge druge, Europska unija potvrđuje da je cyber sigurnost na vrhu evropskih prioriteta. Ali ne samo snažnom izjavom, već i praktičnom spremnošću da se uključe svi resursi i kapaciteti za efikasan odgovor i na fizičke i na cyber prijetnje. Može se zaključiti da ova strategija ima širi utjecaj na zemlje koje teže članstvu u Uniji i nastoje uskladiti svoje zakonodavstvo s evropskim propisima.

Literatura

1.Ангелески М., Криминалистички теории, Скопје, 2014 година.
2.Simonović B., Strateški pristup kriminalističke policije u kontroli kriminala – međunarodni propisi, pojmovno određenje, neki izazovi implementacije, Zbornik radova: Kriminalističko forenzička istraživanja, Vol. 4, br. 1, Banja Luka, 2011 godina.
3.Kozarev A., Uloga Sekretarijata za evropska pitanja Vlade RM u savlađivanju savremenih izazova procesu integracije u EU, Zbornik radova: Evropska unija i Zapadni Balkan – izazovi i perspektive, Institut za međunarodnu politiku i privredu i Hans Seidel Stiftung, Beograd, 2014 godina
4. Kozarev A., Savremeni pristup u borbi protiv organizovanog kriminaliteta u RM, Zbronik radova – VI Naučni skup: Dani bezbjednosti, Univerzitet Sinergija, Banja Luka, 2012 godina.
5. Modly D., ŠuperinaM., Korajlič N., Rječnik kriminalistike, Strukovna udruga kriminalista, Zagreb, 2008 godina.
6.Europska komisija, Komunikacija komisije Europskom parlamentu, Europskom Vijeću, Vijeću, europskm gospodarskom i socijalnom odboru te odboru regija, o strategiji EU-a za sigurnosnu uniju, Bruxelles, 24.07.2020.

https://ec.europa.eu/croatia/News/new_eu_cybersecurity_strategy_and_new_rules_to_make_physical_and_digital_critical_entities_more_resilient_hr, 17.03.2021.
http://morm.gov.mk/wp-content/uploads/2018/07/ns_sajber_bezbednost_2018-2022.pdf, 18