Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

ZLOUPOTREBA SAJBER PROSTORA U IZBORNOM PROCESU KAO GLOBALNA POLITIČKA I SIGURNOSNA PRIJETNJA

ABUSE OF CYBER SPACE IN THE ELECTION PROCESS AS A GLOBAL POLITICAL AND SECURITY THREAT

Pregledni naučni rad

Bakreski Oliver, PhD[428]
Bardjieva Miovska Leta, MS[429]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): Sajber-prostor kao termin dobija potrebnu pažnju zbog svog ogromnog prostora, a istovremeno prazninu, kako za konstruktivne mogućnosti tako i za negativne implikacije.

Ciljevi rada (naučni i/ili društveni): Svrha ovog rada je da analizira i opiše zloupotrebu sajber prostora i sajber aktivnosti i njihovu povezanost sa izbornim procesima. Teorijska implikacija ima za cilj sagledavanje terminoloških odstupanja u smislu upotrebe i zloupotrebe sajber prostora i druge veze sajber bezbjednosti sa izbornim procesom kao globalne političke i bezbjednosne prijetnje.

Metodologija/Dizajn: Primenjena metodologija će omogućiti neophodnu analizu i sintezu otvorenih pitanja vezanih za sajber prostor i njenu zloupotrebu iz suštinskog, pragmatičnog i sadržajnog aspekta.

Ograničenja istraživanja/rada: Ograničenja istraživanja su u domenu institucionalnih kapaciteta za sprečavanje i iskorjenjivanje ovih aktivnosti.

Rezultati/Nalazi: Rezultati ili nalazi sastoje se od opšte situacije i dimenzije sajber prijetnji koje se mogu usmjeriti u samu srž demokratskih procesa.

Generalni zaključak: Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.

Opravdanost istraživanja/rada: Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da

[428] oliverbakreski@yahoo.com
[429] Institut za bezbjednost, odbranu i očuvanje mira. lbardjieva@gmail.com

ima pripremljen plan oporavka od katastrofe kako bi se što pre nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

Ključne reči
bezbjednost, sajber bezbjednost, izbori, strano miješanje, lažne vesti

Abstract
Reason for writing and research problem (s): Sajber-prostor kao termin dobija potrebnu pažnju zbog svog ogromnog prostora, a istovremeno prazninu, kako za konstruktivne mogućnosti tako i za negativne implikacije.
Aims of the paper (scientific and/or social): Svrha ovog rada je da analizira i opiše zloupotrebu sajber prostora i sajber aktivnosti i njihovu povezanost sa izbornim procesima. Teorijska implikacija ima za cilj sagledavanje terminoloških odstupanja u smislu upotrebe i zloupotrebe sajber prostora i druge veze sajber bezbjednosti sa izbornim procesom kao globalne političke i bezbjednosne prijetnje.
Methodology/Design: Primenjena metodologija će omogućiti neophodnu analizu i sintezu otvorenih pitanja vezanih za sajber prostor i njenu zloupotrebu iz suštinskog, pragmatičnog i sadržajnog aspekta.
Research/Paper limitation: Ograničenja istraživanja su u domenu institucionalnih kapaciteta za sprečavanje i iskorjenjivanje ovih aktivnosti.
Results/Findings: Rezultati ili nalazi sastoje se od opšte situacije i dimenzije sajber prijetnji koje se mogu usmjeriti u samu srž demokratskih procesa.
General Conclusion: Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.
Research/Paper Validity: Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da ima pripremljen plan oporavka od katastrofe kako bi se što pre nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

Keywords
security, cyber security, elections, foreign interference, fake news

1. Uvod u sajber bezbjednost i sajber kriminal kao globalnu prijetnju - opće odredbe

Pojam sajber sigurnost, također nazvan informacijska sigurnost, aludira na primjenu integriteta, pouzdanost, poverljivost i dostupnost informacija. Sajber bezbjednost sadrži evoluirajući skup mehanizama, pristupa upravljanju rizikom, tehnologijama, obukom i najboljim praksama dizajniranim da zaštite mreže, uređaje, programe i podatke od napada ili neovlaštenog pristupa.[430]

Merriam Webster rečnik definiše pojam sajber bezbjednosti kao mjere koje se preduzimaju za zaštitu računara ili računalnih sistema od neovlašćenog pristupa ili napada.[431]

Sajber bezbjednost ili bezbjednost informacija su tehnike i tehnologije koje se primjenjuju za zaštitu podataka, računara, mreža i programe od napada i aktivnosti sa svrhom eksploatacije.[432] Sajber bezbjednost se može dalje kategorizovati u sljedećim oblastima: bezbjednost informacija, bezbjednost aplikacija, bezbjednost mreže i oporavak od katastrofe.

Informacijska sigurnost štiti informacije od neovlaštenog pristupa kako bi se spriječila krađa identiteta i kako bi se osigurala zaštita privatnosti. Najčešće tehnike koje se primjenjuju u ovom smjeru su:

- Identifikacija korisnika, autentifikacija i autorizacija
- Kriptografija

Bezbjednost aplikacije obuhvata mjere i kontra mjere koje se primjenjuju tokom razvoja aplikacija i njihovog životnog ciklusa kako bi se zaštitile od prijetnji koje se javljaju zbog nedostataka u dizajnu, razvoju, nadogradnji ili održavanju aplikacije. Osnovne mjere za sigurnost aplikacije su:

- Provjera ulaznih parametara
- Autentikacija i autorizacija korisnika / uloga
- Upravljanje sesijama i manipulacija parametrima i upravljanje iznimkama
- Auditing i logging

---

[430] What is Cyber Security? Cyber Security Defined, Explained and Explored. https://www.forcepoint.com/cyber-edu/cybersecurity (11.05.2019)
[431] Cyber Security. Definition of Cyber Security. Merriam Webster. https://www.merriam-webster.com/dictionary/cybersecurity (07.06.2019)
[432] Definition of "Cyber Security". The Economic Times. https://economictimes.indiatimes.com/definition/cyber-security (05.05.2019)

Sigurnost mreže odnosi se na aktivnosti koje se poduzimaju radi zaštite i osiguranja korištenja, pouzdanosti, integriteta i sigurnosti mreže. Efikasna mrežna bezbjednost pokriva zaštitu od različitih prijetnji i spriječava ih da prodire mrežu ili se šire u njoj. Komponente mrežne sigurnosti su sledeće:

- Anti-virus i anti-spyware
- Zaštitni zid kao blokada za neovlašteni pristup u mreži
- IPS - Sistemi za sprečavanje upada za brzo prepoznavanje prijetnji
- VPN - Virtualne privatne mreže koje pružaju siguran daljinski pristup.

Planiranje oporavka od katastrofe pretpotstavlja proces koji uključuje procjenu rizika, određivanje prioriteta, razvoj strategija oporavka u situacije katastrofe. Svaka institucija i privatnih preduzeća treba da ima pripremljen plan oporavka od katastrofe kako bi se što prije nastavio sa normalnim funkcionisanjem nakon katastrofalnih situacija.

U savremenim uslovima, cyber sigurnost predstavlja značajan aspekt sigurnosti državnih organa, vojske, korporativne institucije, finansijski sektor, kao i zdravstvene ustanove. Organizacije prikupljaju, obrađuju i skladiraju velike količine podataka na računarima i drugim uređajima. Veliki dio ili količina tih podataka može biti osjetljiva informacija, bilo da je riječ o intelektualnom vlasništvu, financijskim podacima, osobnim informacijama ili drugim vrstama podataka za koje neovlašteni pristup ili izloženost mogu imati negativne posljedice.

Organizacije prenose osetljive podatke preko mreža i drugih uređaja u toku poslovanja, a sajber bezbjednost opisuje disciplinu posvećenu zaštiti tih informacija i sistema koji se koriste za obradu ili skladištenje informacija. Šifrovanje je proces kodiranja podataka koji ga čini nerazumljivim i često se koristi tokom prijenosa podataka kako bi se spriječila krađa u tranzitu.

Kao obim i sofisticiranost cyber napada raste, kompanija i organizacija, posebno onih koji su zaduženi za čuvanje informacije koje se odnose na nacionalnu sigurnost, zdravstvenih ili finansijski podaci, potrebno je poduzeti korake kako bi zaštitili svoje osjetljive poslovne i osobne informacije.

U posljednjih nekoliko godina, istaknuto je i naglašeno da cyber napadi i digitalno špijuniranje su vrhu prijetnju nacionalnoj sigurnosti, prevazići čak i prijetnje od napada terorizma.[433]

[433] What is Cyber Security? Definition, Best Practices & More. https://digitalguardian.com/blog/what-cyber-security (04.05.2019).

Izazovi vezani za cyber sigurnost sastoje se od nekoliko elemenata koji definiraju stanje efektivne cyber sigurnosti. Elementi sajber bezbjednosti mogu se opisati na sljedeći način:

- Sigurnost mreže
- Sigurnost aplikacije
- Endpoint security
- Sigurnost podataka
- Upravljanje identitetom
- Sigurnost baze podataka i infrastrukture
- Cloud security
- Mobilna sigurnost
- Planiranje oporavka od katastrofe / kontinuiteta poslovanja
- Obrazovanje krajnjih korisnika

2.1. Elementi sajber bezbjednosti

Snažan položaj sajber bezbjednosti oslanja se na sistematski pristup koji obuhvata sljedeće domene:

- **Sigurnost aplikacije**
  Ranjivosti web aplikacija predstavljaju zajedničku tačku upada za sajber kriminalce. Kako aplikacije igraju sve važniju ulogu u poslovanju, organizacije hitno moraju da se fokusiraju na sigurnost web aplikacija kako bi zaštitile svoje klijente, njihove interese i svoju imovinu.[434]
- **Bezbjednost informacija**
  Informacije su u srcu svake organizacije, bilo da se radi o poslovnim knjigama, ličnim podacima ili intelektualnoj svojini. ISO / IEC 27001: 2013 (ISO 27001) je međunarodni standard koji obezbeđuje specifikaciju za najbolji sistem upravljanja informacijskom sigurnošću (ISMS).
- **Sigurnost mreže**
  Sigurnost mreže je proces zaštite upotrebljivosti i integriteta mreže i podataka. To se obično postiže provođenjem test mrežne penetracije , koji ima za cilj da proceni mrežu za ranjivosti i bezbjednosna pitanja u serverima, hostovima, uređajima i mrežnim uslugama.
- **Planiranje kontinuiteta poslovanja**
  Planiranje kontinuiteta poslovanja (BCP) podrazumijeva pripremu za poremećaj

[434] What are the Biggest Cyber Security Threats in 2019? Forbes. April 2 2019. https://www.forbes.com/sites/quora/2019/04/02/what-are-the-biggest-cybersecurity-threats-in-2019/#21d14d2c4b30 (09.06.2019)

tako što se rano identificiraju potencijalne prijetnje za organizaciju i analizira se kako bi to moglo utjecati na svakodnevne operacije.[435]

- **Operativna sigurnost**
  Sigurnost operacija (OPSEC) štiti osnovne funkcije organizacije praćenjem kritičnih informacija i sredstava koja su u interakciji s njom radi identifikacije ranjivosti.
- **Obrazovanje krajnjih korisnika**
  Ljudska greška ostaje vodeći uzrok kršenja podataka, a strategija sajber bezbjednosti je jaka samo kao najslabija karika. Organizacije moraju biti sigurne da je svaki zaposleni svjestan potencijalnih prijetnji s kojima se suočavaju, bilo da se radi o phishing e-pošti, dijeljenju lozinki ili korištenju nesigurne mreže.
- **Posvećenost liderstvu**
  Posvećenost liderstvu je ključ za uspješnu implementaciju bilo kojeg projekta sajber bezbjednosti. Bez toga je veoma teško uspostaviti, implementirati i održavati efikasne procese. Najviše rukovodstvo mora biti spremno da investira u mjere kibernetičke sigurnosti. viši menadžment treba da da adekvatan prioritet sajber bezbjednosti kako bi podržao dalje ulaganje u tehnologiju, resurse i vještine.[436]

Kada je u pitanju definisanje sajber bezbjednosti i njenih uobičajenih tipova, ove kategorije su označene da suže teorijski pojam i praktičnu primjenu:

- Sigurnost mreže - štiti mrežni saobraćaj kontrolom dolaznih i odlaznih veza kako bi se spriječilo da prijetnje ulaze ili se šire na mreži.
- Prevencija gubitka podataka (DLP) - štiti podatke fokusirajući se na lokaciju, klasifikaciju i praćenje informacija u mirovanju, u upotrebi i u pokretu.
- Cloud Security - pruža zaštitu podataka koji se koriste u uslugama i aplikacijama zasnovanim na oblaku.
- Sistemi za otkrivanje upada (IDS) ili sistemi za sprečavanje upada (IPS) - radi na identifikaciji potencijalno neprijateljske sajber aktivnosti.
- Upravljanje identitetom i pristupom (IAM) - upotreba usluge autentifikacije za ograničavanje i praćenje pristupa zaposlenika radi zaštite internih sistema od zlonamjernih entiteta.
- Antivirus / anti-malware rešenja skeniraju računarske sisteme za poznate prijetnje. Savremena rješenja mogu čak i da otkriju nepoznate prijetnje na osnovu njihovog ponašanja.

---

[435] Three Key Elements of Cyber Security Strategy. *CIO Applications Europe*. December 3 2018. https://www.cioapplicationseurope.com/news/three-key-elements-of-cybersecurity-strategy-nid-484.html (26.04.2019)
[436] Roohparvar, R.: Elements of Cyber Security. *Infoguard Cybersecurity*. March 2 2019. http://www.infoguardsecurity.com/elements-of-cybersecurity/ (28.04.2019)

Zanimljiva činjenica koju treba spomenuti je inicijativa koja omogućava radnicima na daljinu i dovođenje vlastitog uređaja (BYOD)[437] Ovakve politike su proširile perimetar, smanjile vidljivost u sajber aktivnostima i proširile površinu napada.[438]

2. Zloupotreba sajber prostora u koruptivne svrhe - lažne vijesti, namještanje, strano uplitanje, izborno spajanje

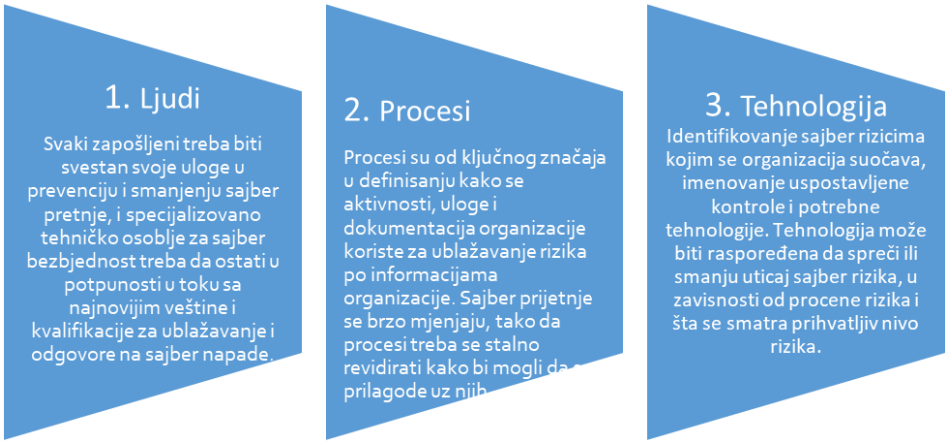
Tradicionalna sajber bezbjednost je centrirana u domenu implementacije odbrambene mjere oko definiranog perimetra. U današnjim događajima, upada u kibernetičkom prostoru rastu brzim tempom, uprkos rekordnim iznosima potrošnje sigurnosti. Jaka sajber sigurnost je ključni odbranbeni sistem vezan protiv sajber kvarova i grešaka i zlonamerne sajber napada, tako da je od vitalnog značaja imati sajber sigurnosne mjere koje štite određene organizacije.[439] Novi propisi i zahtjevi za izvještavanje čine nadzor nad rizikom po sajber bezbjednosti izazov.[440] Da bi se odgovorilo na suvremene prijetnje, organizacije širom svijeta okreću se ljudskoj centricnoj sajber bezbjednosti, novom pristupu koji stavlja fokus na promjene u ponašanju korisnika umjesto eksponencijalnog broja rastućih prijetnji. Ovaj pristup se zasniva na analitike ponašanje.

Humanocentrična sajber bezbjednost pruža uvid u to kako krajnji korisnik stupa u interakciju s podacima i proširuje sigurnosne kontrole u sve sisteme u kojima se nalaze podaci, čak i ako nisu isključivo pod kontrolom organizacije. Na kraju, ovaj pristup je dizajniran da identifikuje anomalije u ponašanju kako bi se izašlo na površinu i odredili prioriteti za najozbiljnije prijetnje, smanjujući vrijeme otkrivanja istraga i prijetnji.

Sajber bezbjednost se može podeliti na tri stuba:

---

[437] Bring your own device (BYOD) refers to employees who bring their own computing devices - such as smartphones, laptops and tablet PCs - to work with them and use them in addition to or instead of company-supplied devices. https://www.techopedia.com/definition/29070/bring-your-own-device-byod (05.06.2019)
[438] Top 15 Cyber Threats for 2019. Cyber Security Insiders. https://www.cybersecurity-insiders.com/top-15-cyber-threats-for-2019/ (10.05.2019)
[439] 8 Cyber Security Risks That May Impact Organizations in 2019. February 13 2019. *Security Magazine*. https://www.securitymagazine.com/articles/89864-cybersecurity-risks-that-may-impact-organizations-in-2019 (18.05.2019)
[440] Discussion Drafts. Cybersecurity Requirements. https://interact.gsa.gov/sites/default/files/Cyber_Risk_Management_Plan_Interact_Release.pdf (01.05.2019)



Cyber napadi postaju sve sofisticiraniji, a taktike i metode koje koriste napadači također se razvijaju i šire u raznolikosti kako bi iskoristile prednosti ranjivosti, među kojima su socijalni inženjering, malware i ransomware. U tom kontekstu, organizacije i institucije će nastaviti da traže garancije od menadžmenta da će njihove strategije za cyber rizik smanjiti rizik od napada i ograničiti finansijske i operativne uticaje.[441]

Ovaj kontekst postavlja pitanje: Koje su posljedice sajber napada? Sajber napadi mogu poremetiti i prouzrokovati znatnu finansijsku i reputacijsku štetu čak i najotpornijoj organizaciji. Ako određena organizacija, institucija ili preduzeće pretrpi cyber napada, oni vjerovatno će se suočiti sa gubitkom imovine, ugleda i poslovanja, i potencijalno će se suočiti sa regulatornim kaznama i parnicama - kao i troškovi sanacije.[442]

Generalno, sajber napadi su počinjeni zbog motive koristi napadača. Oni ulažu u različite tehnike, tehnologije i alate kako bi ostvarili svoje motive. Jedan od najčešćih motiva je finansijska korist, ali sajber napadi može se dogoditi zbog političkim, intelektualnim ili društvenim poticajima.[443]

Tabela 1 : Uobičajeni tipovi kibernetičkih pretnji. Izvor: https://digitalguardian.com/blog/what-cyber-security

[441] UNDP Guidelines on prevention of election violence. The electoral knowledge network. http://aceproject.org/electoral-advice/archive/questions/replies/438369727 (23.04.2019)
[442] The Definition of Cyber Security. IT Governance UK. https://www.itgovernance.co.uk/what-is-cybersecurity (28.05.2019)
[443] 2019 Cyber Security Risk Report. What's Now and What's Next. February 2019. AON's Cyber Solutions. https://www.aon.com/getmedia/4c27b255-c1d0-412f-b861-34c5cc14e604/Aon_2019-Cyber-Security-Risk-Report.aspx (20.05.2019)

Malware	Zlonamerni softver kao što su kompjuterski virusi, špijunski programi, trojanski konji i keyloggeri
Ransomware	Malver koji blokira ili šifrira podatke dok se ne plati otkupnina
Phishing Attacks	Praksa dobijanja osetljivih informacija (npr. Lozinke, informacije o kreditnoj kartici) putem prikrivene e-pošte, telefonskog poziva ili tekstualne poruke
Advanced Persistent Threat	Napad u kojem neovlašćeni korisnik dobija pristup sistemu ili mreži i tamo ostaje duževrijeme bez otkrivanja.
Social Engineering	Psihološka manipulacija pojedinaca za dobijanje povjerljivih informacija; često se preklapa sa phishing-om.

3. Sajber bezbjednost u izbornom procesu

Pravični izbori predstavljaju okosnicu demokratije. Kredibilitet organizovanja izbora, kampanja, ishoda i implementacije u velikoj mjeri zavisi od primijenjenih metoda i tehnika glasanja. Tokom ljudske egzistencije u istoriji, izbori su sprovođeni na gravirane ploče, kuglice u boji ili grahu, papirnim glasačkim listićima, mehaničkim polugama, optičkim skenerima, perforiranim karticama, računarima i kompjuterskom softveru, internet glasanju itd.[444] Svrha ovog rada je da naglasi potrebu za organizovanjem sigurnih izbora koji će garantovati vladavinu prava i poštovanje demokratskih principa državne uprave. Izbori predstavljaju osnovu za uspostavljanje vlade, a oni imaju značajnu ulogu u određivanju strateškog stanovišta na kojem će zemlja poduzeti korake u pogledu unutrašnjih i vanjskih poslova, ekonomije, socijalnih politika, vladavine prava i sigurnosti i stabilnost. Ograničenja u istraživanju su u domenu institucionalnih kapaciteta za obezbjeđivanje optimalnog nivoa održavanja izbora na demokratski način, uz transparentnu kampanju, sprečavanje širenja propagande i lažnih izvora vijesti i web stranica.[445]

Strano uplitanje, sumnjivo finansiranje kampanja, namještanje izbora, izborne prevare, širenje lažnih vijesti i spinova samo su neki od faktora koji mogu potkopati izborne procese i čak stvoriti plamište za izborno nasilje. U tom pravcu, diskusija o strategija prevencije koje bi se mogle provesti kako bi se ublažilo izborno nasilje prvo zahtijeva

[444] Helios: Web-Based Open-Audit Voting. 17th USENIX Security Symposium. http://static.usenix.org/event/sec08/tech/full_papers/adida/adida.pdf (30.05.2019)
[445] A Handbook for Elections Infrastructure Security. Center for Internet Security. CIS. Version 1.0 february 2018. https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf (19.04.2019)

identifikaciju različitih vrsta izbornog nasilja koje može doći ako je identifikovano sajber sigurnosnu prijetnju ili ako sajber napad prekine izbornog procesa.[446]

Ovaj nalaz ukazuje na potrebu razlikovanja nasilja koje ima za cilj ometanje izbora od strane aktera koji uopće ne žele da se izbori održe, i nasilje izazvano rivalstvom između kandidata / stranaka koje se natječu. Ako dođe do prvi vid nasilja, nacionalnih snaga sigurnosti može se mobilizirati i ciljaju opstrukcionisti, što dovodi do pažnju na navedenih vrste sukoba, gdje neke stranke se ne slažu o tome da li ili kada će održati izbore, što izaziva njihovi motivi za razmatranje i izvršenje sajber napada i drugih oblika izbornog ometanja. Kada se analizira i procjeni razlog i motivi za aktivno prekidanje procesa glasanja spojler grupa zbog straha od gubitka moći ili u svrhu mijenjanja rezultata i ishoda, te je s odbijanjem da učestvuju na izborima, treba uzeti u obzir prethodni razvoj ili oblik ranije pregovore .[447] Da li se radi o širem političkom, geopolitičkom, sekuritizovanom procesu, sklonom stranom uplitanju i elementima proxy hibridnog uticaja, i rezultatima izbora koji će imati širi uticaj na političku, ekonomsku i bezbjednosnu klimu na regionalnom i međunarodni nivo.[448]

Pored toga, vrijedno je naglasiti povezanost između sajber bezbjednosti i bezbjednosti izbora sa činjeničnom nasilnom eskalacijom. Posebno u smislu nedovoljnog institucionalnog kapaciteta, postoji mogućnost transformacije prijetnje, počevši od kibernetičke prijetnje i odvijajući se kao nasilni nemiri koji dovode do žrtava, materijalne štete i gubitka poverenja. Kada je riječ o analizi izbornog nasilja tokom izbornog procesa, može se podijeliti na određene komponente, uključujući:

- motivi,
- žrtve,
- počinioci,
- odgovora, kao i
- uticaja nasilja.

Posljednjih godina, paralelno sa razvojem IT sistema i mrežnih tehnologija, mnoge zemlje su uvele elektronske glasačke listiće i softverske programe u cilju sprovođenja izbornog procesa. Računarski uređaji za glasanje mogu se definirati kao digitalni model tradicionalnog glasačkog modela glasačkih listića. One predstavljaju dostupnost, pouzdanost, upotrebljivost i provjerljivost sistema e- glasanja. Ali, ima još toga, jer su te tehnologije po

[446] Elections Cyber Security. Center for Democracy and Technology. https://cdt.org/issue/internet-architecture/election-cybersecurity/ (08.05.2019)
[447] Ellena, K., & Petrov, G. (2018). Cyber Security in Elections. Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. http://aceproject.org/ero-en/ifes-cybersecurity-in-elections (21.05.2019)
[448] Election Cyber Security. Politico LLC. 2019 https://www.politico.com/tag/election-cybersecurity (01.06.2019)

prirodi ranljive i predstavljaju sigurnosni izazov. To znači da su računari i programi za glasanje pod prijetnjom hakiranja i manipulacije kako bi se kompromitovao integritet izbora od strane treće strane.[449]

U tom pravcu, razvijena je praktično primjenljiva enkripcija koja obezbjeđuje siguran sistem za glasanje zasnovan na kriptografiji bez curenja . Ovo pretpostavlja tajne potvrde o glasanju koje sprečavaju uplitanje treće strane, kao i efektivno eliminišu mogućnost za prodaju, kupovinu i prinudu glasa. Ovaj dizajn enkripcije razvijen na anonimnom kanalu ili kaskadnoj mreži se zove *semantički siguran*. Time se osigurava privatnost birača, sprečavanje kupovine, prodaje ili prisile glasača, kao i osiguravanje integriteta glasačkih listića i provjerljivost glasova.[450]

Što se tiče izbornog procesa, kompjuterski glasački sistemi mogu biti hakirani, oteti ili narušeni ovim sredstvima:

- Malver korišćen za promjenu glasova unutar digitalnih glasačkih mašina
- Zlonamjerni softver umetnut na osobnim računalima radi promjene glasova na online izborima
- Poremećeni DDoS napadi na izborne servere
- Lažne izborne internet stranice i zavaravanje birača[451]

Ograničenje i nemogućnost za efikasnu zaštitu od izbornih sajber napada, iskorenjivanje stranih izbornih miješanja, i tako dalje, proizlazi iz brojnih faktora koji su u pitanju. One obuhvataju različite dimenzije, kao što su instalacija i rad bot centara koji šire zlonamjernih programa, lažne vijesti, propagandu ili klasificirane informacije, koje su komplicirane za lociranje od strane odgovarajućih sektora ministarstva unutrašnjih poslova; korupcije na visokom nivou u samoj zemlji sa višeslojnim vezama sa predstavnicima stranih zemalja, itd.

Izborni proces predstavlja značajan demokratski čin za postizanje političke moći mirnim putem i ovaj proces u savremenom okruženju je ranjiv u nekoliko aspekata u pogledu bezbednosti. Prijetnja sajber napadom izbornih podataka, hakerski upadi na zvanične web stranice, kao i širenje lažnih novosti i propagande na internetu ugrožava izborni proces u svakoj fazi. Čak i prije početka zvanične kampanje, kao i tokom perioda nadzora i

[449] Nemati, R., H., Yang, L. (2011): Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. New York, Information Science Reference.
[450] Handbook for the Observation of New Voting Technologies. OSCE/ODIHR 2013, Warsaw Poland. https://www.osce.org/odihr/elections/104939?download=true (09.06.2019)
[451] Zetter, K.: The Crisis of Election Security. *The New York Times Magazine*. September 26 2018. https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html (11.05.2019)

ispravki biračkih spiskova, i sve do prebrojavanja glasova i rezimiranja rezultata nakon završetka ankete, rizik ostaje prisutan.

Izbori su borba za legitimnu vlast koja se može opisati kao nenasilna konkurencija, koja se vodi u okviru političkog foruma. U ovom kontekstu, važno je prepoznati da izbori ne izbjegavaju konfrontaciju, već se fokusiraju na upravljanje i ograničavanje unutar prihvaćenih granica. U praksi, osiguranje pravične sigurnosti tokom izbornog procesa je od suštinskog značaja za zadržavanje poverenja i predanosti učesnika izborima. Shodno tome, bezbjednost je i sastavni deo cilja izbora i neodvojivi dio izbornog procesa. Ne postoji jedinstveni model izbora ili demokratije koji je univerzalno primjenjiv na sve zemlje. Izbor je jedinstven; definisan ne samo izbornim pravilima, već i društvenim vrijednostima, politikom, religijama, istorijom i kulturom naroda. Na isti način, bezbjednost izbora je jedinstvena za okolnosti u kojima se sprovodi. Ulozi pojedinih izbora su različiti, čak i ako se periodično održavaju u istoj zemlji, zbog promjenljivih sila koje oblikuju nacionalni interes i odgovarajuću političku agendu.[452]

Kada se govori o sigurnosti i sigurnosti izbora i pouzdanosti izbora, pravni aspekt mora biti označen na odgovarajući način. Znači, postoje brojni standardi koji su uvedeni na međunarodnom nivou, ali još mnogo toga treba uraditi kako bi se one u potpunosti implementirale i prilagodile sve većim prijetnjama i izazovima u pogledu sigurnosne dimenzije izbora. Usvojeni standardi su sljedeći:

- The Universal Declaration on Human Rights. Article 21, Paragraph (3). UN General Assembly Resolution 217A
- ICCPR - International Covenant on Civil and Political Rights Resolution 2200A (XXI) (Article 25) adopted by the General Assembly of the United Nations
- UN General Assembly Guidelines for the Regulation of Computerized Data Files (1990). Resolution 45/95
- UN Resolution 34/7. The right to privacy in the digital age. UN Privacy and Data Protection Principles (2017)[453]
- Recommendation CM/REC (2017)5 of the Committee of Ministers to member states o standards for e-voting Council of Europe e-voting standards (2017): Appendix I, Section VIII. Reliability and Security of the System
- Open Government Declaration (2011) Global Report 2019. Democracy Beyond the Ballot Box

Izbor kao demokratski instrument ima snažan potencijal koji se širi i izvan političkih implikacija. Razvoj društva i rastuća interakcija i složenost ljudskih aktivnosti nameću potrebu za odgovarajućim rješenjem u pogledu održavanja modernih izbora. Uključujući značajnu

[452] Council of Europe: E-Voting. https://www.coe.int/en/web/electoral-assistance/e-voting (12.05.2019)
[453] Election Technology and Cyber Security: Standards, Good Practice and Guidelines. The Electoral Knowledge Network. http://aceproject.org/election-technology-and-cyber-security-standards (23.04.2019)

predizbornu kampanju, siguran proces glasanja, precizan i provjerljiv broj glasova i adekvatnu implementaciju izbornih rezultata. Osiguranje sigurnosnog aspekta ovog značajnog akta je imperativ za savremena društva. U tom pravcu su nastojanja da se uspostave univerzalni standardi i sigurnosne procedure i mjere za garantiranje pouzdanog ishoda.[454]

Ipak, uprkos trendovima inicijativa za e-glasanje, proces implementacije se odvija sporije nego što se očekivalo, a to je zbog nekoliko faktora koji uključuju tehničku, socijalnu i kulturnu dimenziju. Paralelno s tim, harmonizacija sistema elektronskog glasanja, u okviru različitih zakonskih i statutarnih oznaka, također predstavlja izazov koji ostaje da se prevlada.

Izborna 'namještanja' ili percipirano namještanje izbora mogu uzrokovati nasilje, ali nasilje je često samo oblik namještanja. Prilikom ispitivanja veza između namještanja i nasilja, važno je uočiti evoluciju namještanja, manipulacije ili iskrivljavanja rezultata tokom posljednjih godina i razmotriti šta se može učiniti kako bi se to riješilo. Treba identifikovati odnose između državnih resursa i namještanja, nasilja i namještanja.[455]

Ne postoji univerzalna definicija "izborne prijevare", jer se ona razlikuje u vremenu i na različitim lokacijama. Drugi izrazi koji se koriste kao zamjena za prijevaru su zloupotreba, nedolično ponašanje, nepravilnosti i manipulacija. Izborna prijevara podrazumijeva samo obmanu, ali ne i svi izborni zločini uključuju samo varanje. Postoje i prakse koje nisu same po sebi nezakonite, ali nisu u skladu sa međunarodnim standardima. Ove nezakonite prakse uključuju sljedeće:

- sprečavanje birača da popune glasačke listiće,
- netačna kampanjska literatura,
- prisilno povlačenje protivnika (a),
- plačanja olakšice, i
- propuste u dužnoj pažnji izbornih zvaničnika.[456]

[454] Election Security. Homeland Security. https://www.dhs.gov/topic/election-security (23.05.2019)
[455] Elections – Critical Infrastructure. US Election Assistance Commission. https://www.eac.gov/election-officials/elections-critical-infrastructure/ (25.05.2019)
[456] Fiddler, D., P.: Policy Dimensions of Strenghtening Elections Cybersecurity. Council on Foreign Relations. October 18 2017.
https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_182365.pdf (01.06.2019)

Kako bi se utvrdio nivo i tip ranjivosti koje postoje, procjena rizika za izborni kriminal bi trebala biti provedena od strane relevantnih tijela . Procjena historije izbornih namještanja može ukazati na potencijalnu veličinu i utjecaj na ishode.[457] Može se identifikovati:

- mjesta na kojima se očekuje da će se dogoditi zločini,
- u kojoj fazi izbornog ciklusa mogu se desiti, i
- da li su zločini vjerovatno epizodni ili sustavni.[458]

Unutar izbornog ciklusa, rizik se može identificirati kao da se odvija u sljedećim fazama:

- identifikaciju i registraciju birača,
- politička kampanja,
- glasanje na dan izbora,
- transport osjetljivih izbornih materijala,
- tabeliranje glasovanja, i
- adjudikacija i sertifikacija.[459]

Ovi obrasci su na raspolaganju vladinim institucijama, izbornim komisijama, sigurnosnim snagama, kao i drugim uključenim akterima, kako bi se implementirala alternativa koja će u konačnici spriječiti ili ublažiti daljnje izborno nasilje.[460]

4. Zaključak

Što se tiče nalaza i elaboriranih podataka u ovom radu, četiri hipoteze se mogu izvući kao zaključci.

Prva tvrdnja je sve veća dimenzija bezbjednosti kao stanje i cilja - koja obuhvata domenu sajber bezbjednosti. To pretpostavlja da sajber bezbjednost i alati za osiguranje njenog uključivanja u integralni aspekt upravljanja sigurnošću idu ruku pod ruku sa ekonomskom sigurnošću, kritičnom bezbjednošću infrastrukture, političkom stabilnošću itd.

---

[457] Lin, H.: Election Hacking, As We Understand it Today, is not a Cyber Security Issue. January 5 2018. *Lawfare*. https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue (11.06.2019)

[458] EU Member states Test Their Cyber Security Preparedness for Fair and Free 2019 EU Elections. European Commission. http://europa.eu/rapid/press-release_IP-19-2011_en.htm (19.05.2019)

[459] H2020 – EU 3.7.4. – Improve Cyber Security. https://cordis.europa.eu/programme/rcn/664471/en (12.06.2019)

[460] Elections, Violence and Conflict Prevention. European Commission United Nations Developing Programme. Joint Task Force on Electoral Assistance. June 2011. https://www.undp.org/content/dam/brussels/docs/Other/JTF%202011.06_Summary_report-Barcelona_workshop_Elections&conflict.pdf (24.04.2019)

Druga tvrdnja koja proizilazi iz analiziranih podataka u ovom radu sumira aspekt upravljanja sajber bezbjednošću i procenu rizika sajber sigurnosti. Upravljanje od top menadžmenta do nižeg nivoa je nosilac inicijativa za sajber bezbjednost i davanje prioriteta ovom pitanju u okviru organizacije ili korporacije. Kada je u pitanju upravljanje sajber bezbjednošću i zaštitom podataka u datom preduzeću, procene sajber rizika fokusiraju se na tri ključna aspekta:

1. Identifikacija najvrednijih podataka organizacije koji zahtijevaju zaštitu,
2. Identificiranje rizika i prijetnji u pogledu njegove zaštite i
3. Označavanje štete nanesene u slučaju gubitka podataka ili nezakonite izloženosti.

Treći zaključak iz ove hipoteze odnosi se na potrebu stvaranja i pridržavanja propisa kada je u pitanju prikupljanje, čuvanje i sigurnost podataka. Ova razmatranja treba da se urade i u pravcu procene rizika. Kao pravni odgovor na rastuće pitanje vezano za sajber bezbjednost i temeljno pravo na prirodnu privatnost i zaštitu podataka, Evropski parlament i Vijeće izdali su uredbu EU 2016/679 (Direktiva 95/46 / EZ o općoj uredbi o zaštiti podataka).[461]

Kada je u pitanju rješavanje pitanja vezanih za sigurnost, Direktiva Član 19. definiše da zaštita fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa u svrhu sprečavanja, istrage, otkrivanja ili krivičnog gonjenja krivičnih djela ili izvršenja krivičnih sankcija, uključujući zaštitu od i sprečavanje prijetnji javnoj sigurnosti i slobodno kretanje takvih podataka, predmet je posebnog pravnog akta Unije. Stoga se ova Uredba ne bi trebala primjenjivati na aktivnosti obrade u te svrhe. Međutim, lični podaci koje obrađuju javni organi prema ovoj Uredbi trebali bi se, kada se koriste u te svrhe, regulirati specifičnijim pravnim aktom Unije, naime Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća.

Četvrti zaključak povezan je sa sajber bezbjednošću i izborima. Od predsjedničkih izbora u SAD 2016. godine i Mueller-ovog izvještaja o istrazi o ruskom uplitanju doveli su do kontroverzi i izazvali debatu i sumnju u ranjivost prema izbornim procesima i rezultatima, sajber bezbjednost na izborima dobila je središte pažnje u organizaciji i održavanju izbora u mnogim zemljama u svijetu.

[461] The EU General Data Protection Regulation (GDPR). 2018 Reform of Data Protection Rules. European Commission. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en (30.05.2019)

5. Literatura:

1. Ayala, L. (2016): Cyber Security Lexicon. New York, Springer Science and Apress.
2. Delta, G., B., Matsuura, J., H. (2019): Law of the Internet, Fourth Edition. Volume 1, Supplement. New York, Wolters Kluwer.
3. Goldstein, M., J., Gitlin, M.. (2015): Cyber Attack. Minneapolis, Twenty First Century Books.
4. Hackett, R. (2018): Cyber Security: Hacking, the Dark Web and You. Tampa, FL, Time Books Edition.
5. Heitkamp, K., L. (2019): Interference in Elections. New York, Greenheaven Publishing.
6. Kamar, H. (2018): What is Cyber Security? New York, Britannica Educational Publishing.
7. Li, K, Chen, X., Susilo, W. (2019): Advances in Cyber Security: Principles, Techniques and Applications. Singapore, Springer Nature.
8. Lucas, G. (2017): Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Madison Avenue, New York, Oxford University Press.
9. Nemati, H., R., Yang, L. (2011): Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering. Hershey New York, Informational Science Reference.
10. Norris, P. (2017): Strengthening Electoral Integrity. Cambridge, Cambridge University Press.
11. Norris, P., Cameron, S., Wynter, T. (2019): Electoral Integrity in America: Securing Democracy. New York, Oxford University Press.