

## NACIONALNA BEZBEDNOST – ULOGA DRUŠTVENIH MREŽA\*\*\*

**Sažetak:** Društvene mreže su uplivale u sve sfere modernog društva. Omogućavaju onlajn povezivanje korisnika sa svojim prijateljima i porodicom, istraživanje potrebnih informacija, zabavu, ali i onlajn kupovinu. Sve je češća upotreba sajtova društvenih mreža i od strane kompanija za komunikaciju sa ciljnim tržištem, ali i same vlade postaju svesne njihove upotrebne moći. Međutim, kao relativno još uvek neuređena oblast (pre svega zakonski), društvene mreže su mesto gde se sve češće odvijaju aktivnosti sajber napadača, koje mogu ugroziti kako bezbednost pojedinaca tako i same države. Sve je više primera u kojima sajber teroristi upotrebom sajtova društvenih mreža, šire dezinformacije, ideologiju, izazivaju strah, ali i regrutuju svoje pristalice, čime direktno ugrožavaju nacionalnu bezbednost. Sa druge strane, društvene mreže mogu u isto vreme biti i veoma korisno sredstvo za zaštitu nacionalne bezbednosti, kao veoma efikasno oruđe za komunikaciju sa stanovništvom u situacijama kada je važno brzo upozoriti ljude na potencijalnu opasnost od terorističkog delovanja.

**Ključne reči:** Društvene mreže, Nacionalna bezbednost, Sajber napadači, Sajber terorizam

### 1. UVOD

Kada govorimo o bezbednosti, uobičajeno je da se ona vidi u realnoj perspektivi, a to je da je bezbednost „stanje bez ikakve pretnje“. Osećaj sigurnosti se može postići eliminacijom pretnji ili posredovanjem dovoljno sopstvenih resursa da se čovek može osetiti sigurnim od pretnji.<sup>1</sup> Literatura o definicijama nacionalne bezbednosti je obilna i još uvek raste.<sup>2</sup> Stoga je uobičajeno videti da se u različitim definicijama spominje ljudska bezbednost, nacionalna bezbednost, međunarodna bezbednost, bezbednost režima, korporativna bezbednost, iz-

\* Docent, Pravni fakultet, Megatrend univerzitet, nikoleta.lutovac@yahoo.com

\*\* Vanredni profesora, Pravni fakultet, Megatrend univerzitet, sveto.lutovac@gmail.com

\*\*\* Rad je rezultat Projekta Pravnog fakulteta FPBISD Bezbednosni izazovi savremenog društva.

<sup>1</sup> Više o tome: Christiansson, M. (2004): Säkerhetspolitisk teori, 1. ed., Stockholm: Militärhögskolan Karlberg.

<sup>2</sup> Oche, O. (2005): Low Intensity Conflicts, National Security and Democratic Sustenance, in Saliu, H A. (ed.) Nigeria under Democratic Rule 1999-2003, Ibadan University, Ibadan.

među ostalog.<sup>3</sup> Danas se sprovodi mnogo istraživanja iz sočiva bezbednosti, koji analiziraju potencijalne sajber pretnje kojima društveni mediji mogu učiniti pojedince i organizacije podložnim sajber napadima. Očekuje se da će nova istraživanja koja se fokusiraju na društvene mreže biti usmerena na integraciju tehnologije, kao što su blokčejn, veštačka inteligencija, kriptovaluta i proširena stvarnost.<sup>4</sup>

Društvene mreže imaju ogroman uticaj i utiču na čitave kulture i poslovne procese,<sup>5</sup> sa širim socio-ekonomskim implikacijama društvenih medija, što znači da je sadržaj društvenih medija ključan za makroekonomski i kulturni razvoj. Obim, brzina i obim podataka koje obrađuju platforme društvenih medija u najkraćim denominacijama čine ih ključnom brigom za studije nacionalne bezbednosti.<sup>6</sup> Upotreba interneta i društvenih mreža za terorizam uključuje planiranje sajber napada, širenje ekstremističkih ideologija i propaganda, ali i regrutovanje istomišljenika. Prednost koju teroristički aktivisti vide u korišćenju ovakvih tehnika je nesumnjivo sposobnost da se održi anonimnost i da se lako pronađu skrovišta u širokom sajber prostoru.<sup>7</sup>

## 2. NACIONALNA BEZBEDNOST: DEFINISANJE I KONCEPTUALIZACIJA

Izraz bezbednost po svom etimološkom poreklu potiče od latinskog *securus*, što znači bez straha, a upućuje nas na odsustvo rizika, predvidljivosti i izvesnosti u pogledu budućnosti. Kako kaže Filip Dejvid (Philippe David), koncept bezbednosti je bio predmet duboke konceptualne obnove, s obzirom na kapacitet države da obuzda pretnje svom suverenitetu, usled evolucije klasičnih nivoa analize nacionalnih, regionalnih, međunarodnih i kooperativna bezbednost, na nivo zajedničke, globalne i ljudske bezbednosti.<sup>8</sup> Koncept je time izgubio gotovo isključivo javnu, nacionalnu i vojnu dimenziju.<sup>9</sup> Dakle, koncept nacionalne bezbednosti sastoji se od: situacije koja garantuje jedinstvo, suverenitet i nezavisnost nacije; integritet teritorije i bezbednost lica i robe; jedinstvo države i normalan razvoj njenih zada-

<sup>3</sup> Waever, O. (1995): *Securitization and Desecuritization*, in Lipschutz, R.(ed.), *On Security*, Columbia University Press, New York, pp. 46-86.

<sup>4</sup> Choi, T. M., Guo, S. & Luo, S. (2020): *When blockchain meets social- media: Will the result benefit social media analytics for supply chain operations management?* *Transportation Research Part E: Logistics and Transportation Review*, 135, 101860.

<sup>5</sup> Cao, Y., Ajjan, H., Hong, P. & Le, T. (2018): *Using social media for competitive business outcomes.* *Journal of Advances in Management Research*, 15(2), pp. 211–235.

<sup>6</sup> Huang, S.Y. & Ban, T. (2020): *Monitoring social media for vulnerability: Threat prediction and topic analysis.* In: *Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications*, Guangzhou, January 2021. New York: IEEE, pp. 1771–1776.

<sup>7</sup> Baltezarević, R. & Baltezarevic, I. (2023): *Terorizam u digitalnom okruženju.* *Baština*, Vol. 33 sv. 60, pp. 173-181 doi: <https://doi.org/10.5937/bastina33-44435>

<sup>8</sup> Više o tome: Charles-Philippe, D. (2001): *A Guerra e a Paz: Abordagens contemporâneas da Segurança e da Estratégia.* Lisbon: Instituto Piaget.

<sup>9</sup> Više o tome: Guedes, M. & Elias, L. (2010): *Controlos Remotos Dimensões Externas Da Segurança Interna Em Portugal.* Coimbra: Almedina.

taka; sloboda političkog delovanja organa suvereniteta i redovno funkcionisanje demokrat-  
skih institucija sadržanih u ustavnom okviru.<sup>10</sup>

Nacionalna bezbednost ima i kvalitativnu i dinamičku dimenziju. Kvalitativno ona obuhvata beskrajni nagon države za poboljšanjem bezbednosti i zaštitom života, imovine i resursa unutar definisanih teritorijalnih granica. Dinamična je u smislu da njene konture osciliraju sa pojavom novih pretnji ili transformacijom starih pretnji, koje mogu doći unutar ili izvan njenih teritorijalnih granica.<sup>11</sup> Kao što se menjaju politički, ekonomski, vojni i društveni uzroci pretnji, tako se menja i položaj nacionalne bezbednosti zemlje.<sup>12</sup> Tvrđnja da je vestfalska država bila početak nacionalne bezbednosti mogla bi da izazove izvesnu kritiku od strane studenata istorije, uzimajući u obzir rane gradove-države i imperije koje su bile više nego sposobne da iskoriste silu i da se brane.<sup>13</sup> Ipak, važno je napomenuti da je nacionalna komponenta nacionalne bezbednosti povezana sa državom. Pitswane (Pitswane) tvrdi da su ključni elementi nacionalne bezbednosti vojna moć, teritorijalni opstanak države i suverenitet. Objašnjenje nacionalne komponente je takva da je bezbednost države morala da se brani od pretnji.<sup>14</sup> U ovom kontekstu, treba razumeti da kada se radi o nacionalnoj bezbednosti, postoji pretnja po bezbednost države. U tradicionalnom ili realističkom smislu to je logično, jer je država centralna i glavna, a nacionalna bezbednost je najvažniji faktor.<sup>15</sup> Buzan i Hansen (Buzan & Hansen) smatraju da je nacija/država uvek bila analitički i normativni referentni objekat i da se obezbeđivanjem države mogu obezbediti i drugi referentni objekti, a drugi autori su приметili da nacionalnu bezbednost zapravo treba nazvati državnom bezbednošću.<sup>16</sup>

Terif i dr. (Terrif) navode da je bezbednost osećaj sigurnosti od štete ili opasnosti.<sup>17</sup> Džekson-Pris (Jackson-Preece) klasifikuje bezbednost kao osnovnu vrednost ljudskog života.<sup>18</sup> Vilijams (Williams) ukazuje da je bezbednost povezana sa pretnjama negovanim vrednostima, koje mogu ugroziti određeni referentni objekat u budućnosti.<sup>19</sup> Braun (Brown) tvrdi, da je nacionalna bezbednost sposobnost očuvanja fizičkog integriteta i teritorije nacije; da održava svoje ekonomske odnose sa ostatkom sveta pod razumnim uslovima; da zaštititi

<sup>10</sup> Ibid

<sup>11</sup> Onuoha, F. C. (2008): Oil pipeline sabotage in Nigeria: Dimensions, actors and implications for national security. *African Security Review*, Vol.17, No.3, pp. 98-115.

<sup>12</sup> Okodolor, C. (2004): National security and foreign policy: towards a review of Nigeria`s afro-centric policy. *Nigerian Forum*, Vol. 25, Nos. 7-8, pp: 204-223

<sup>13</sup> Više o tome: Buzan, B. & Little, R. (2000): *International systems in world history; remaking the study of international relations*. Oxford: Oxford University Press.

<sup>14</sup> Pitswane, J. (1993): Recognizing the non-military dimensions of national security: an agenda for the 1990s. *Peace Research*, 25(4):31-38.

<sup>15</sup> Više o tome: Viotti P.R. & Kauppi, M.V. (1999): *International relations theory: realism, pluralism, globalism and beyond*. Boston: Allyn and Bacon.

<sup>16</sup> Više o tome: Buzan, B. & Hansen, L. (2009): *The evolution of international security studies*. New York: Cambridge University Press.

<sup>17</sup> Više o tome: Terrif, T., Croft, S., James, L. & Morgan P.M. (1999): *Security studies today*. Malden, Massachusetts: Blackwell Publishers incorporated.

<sup>18</sup> Više o tome: Jackson-Preece, J. (2011): *Security in international relations*. London: University of London, London School of Economics and Politics.

<sup>19</sup> Više o tome: Williams, P.D., ed. (2008): *Security studies an introduction*. New York: Routledge.

svoju prirodu, institucije i upravljanje od ometanja spolja; i da kontroliše svoje granice.<sup>20</sup> Većina autora prilično dosledno definiše nacionalnu bezbednost kao sposobnost održavanja fizičkih granica, ekonomskih odnosa i društvenih institucija nacije od spoljnih pretnji. Oblast studija bezbednosti bila je usko definisana tokom Hladnog rata i fokusirana prvenstveno na vojna pitanja. Buzan, Viver i De Wilde (Buzan, Wæver & De Wilde) tvrde da se obim mora proširiti kako bi bolje odražavao širinu pitanja koja imaju uticaj na oblast bezbednosti. Međutim, oni su ovu ekspanziju ograničili tvrdnjom da svaki dodatak mora predstavljati „egzistencijalnu pretnju referentnom objektu“, a ne samo redovno političko pitanje.<sup>21</sup> Može se tvrditi da bez obzira na nivo napora koji se ulažu, mere nacionalne bezbednosti nikada ne mogu garantovati bezbednost svakog pojedinca, entiteta, institucije i artefakta u vlasništvu države. Pored aksiomske nesposobnosti da se stalno zaštite svi ljudi i imovina, nacionalna bezbednost može biti dovedena u pitanje ograničenjima resursa i kriterijumima za određivanje prioriteta, koji podrazumevaju kompromise između troškova i koristi u praktičnim odlukama u vezi sa raspoređivanjem resursa nacionalne bezbednosti. U jednom ili drugom aspektu, nacionalna bezbednost će neizbežno imati slabosti koje čine naciju ranjivom na spoljne ili domaće pretnje.<sup>22</sup>

### 3. ULOGA DRUŠTVENIH MREŽA U NACIONALNOJ BEZBEDNOSTI

Definicija društvenih mreža se promenila od njihovog nastanka. U svojim ranim danima, društvene mreže su bile veb lokacije na kojima su korisnici mogli da kreiraju nalog i povežu se sa drugim korisnicima društvenih mreža.<sup>23</sup> Najčešća upotreba društvenih mreža bila je stvaranje onlajn mreže prijatelja, porodica, vršnjaka, poznanika i ljudi sa zajedničkim interesima.<sup>24</sup> Postepeno su veb stranice i poslovni profili počeli da se uključuju u sajtove društvenih mreža. Ovo je omogućilo korisnicima da komuniciraju sa preduzećima i omogućilo preduzećima da se angažuju sa potrošačima.<sup>25</sup>

Društvene mreže su sveprisutne u modernom vremenu. Razmena informacija, ideja i mišljenja, kulturna svest, diverzifikacija, globalizacija i blagodat industrijalizacije u kontekstu e-trgovine i inovativnih tehnologija može se povezati sa društvenim mrežama.<sup>26</sup> Na

<sup>20</sup> Više o tome: Brown, H. (1983): *Thinking about National Security*. Boulder, CO: Westview.

<sup>21</sup> Više o tome: Buzan, B., Wæver, O. & De Wilde, J. (1998): *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Publishers.

<sup>22</sup> Christensen, T., Læg Reid, P. & Rykkja, L.H. (2015): The challenges of coordination in national security management: The case of the terrorist attack in Norway. *International Review of Administrative Sciences*, 81(2), pp. 352–372.

<sup>23</sup> Van Heekeren, M. (2020): The curative effect of social media on fake news: A historical re-evaluation. *Journalism Studies*, 21(3), pp. 306–318.

<sup>24</sup> Thaer Majali, M.A., Omar, A. & Alhassan, I. (2021): Social media use as health awareness tool: A study among healthcare practitioners. *Multicultural Education*, 7(2), pp. 1-5.

<sup>25</sup> Olanrewaju, A.S.T., Hossain, M.A., Whiteside, N. & Mercieca, P. (2020): Social media and entrepreneurship research: A literature review. *International Journal of Information Management*, 50, pp. 90–110.

<sup>26</sup> Mention, A.L., Barlatier, P.J., & Josserand, E. (2019): Using social media to leverage and develop dynamic capabilities for innovation. *Technological Forecasting and Social Change*, 144, pp. 242–250.

individualnom nivou, sajтови društvenih mreža služe kao platforma za društvenu interakciju, traženje informacija, razmenu informacija i mišljenja i slobodno vreme, Pored toga, preduzeća koriste društvene medije za onlajn trgovinu, brendiranje, marketing, promocije, angažovanje potrošača i usluge korisnicima.<sup>27</sup> Vlade su takođe u mogućnosti da značajno iskoriste društvene mreže, vršeći objavu javnih usluga na sajtovima društvenih mreža, više se angažujući sa građanima, podižući svest o pitanjima javnog zdravlja, promovišući obrazovanje, obezbeđujući karijerno vođenje i olakšavajući e-trgovinu.<sup>28</sup>

Međutim, zbog dinamične prirode aplikacija društvenih mreža, korisnici su identifikovali nedostatke u smernicama i politikama, što dozvoljava eksploataciju i malverzacije. Utvrđeno je da su složeni problemi kao što su maltretiranje putem interneta, zloupotrebe socijalnog inženjeringa kao što je pecanje (phishing) i lažne aktivnosti kao što je prevara, prevladavajuće u nekoliko zajednica društvenih mreža.<sup>29</sup> Iako ova pitanja predstavljaju rizik za osobu ili organizaciju, društvene mreže takođe predstavljaju rizik od manipulacije velikih razmera koje mogu da dovedu naciju u opasnost. Od političkih ciljeva, špijunaže i klevete uticajnih i istaknutih ličnosti do dela međunarodnih zločina, uključujući sajber terorizam, sajber rat, hibridni rat, pretnje socijalnoj sigurnosti građana, regrutovanje špijuna i masovno širenje dezinformacija, sajтови društvenih mreža mogu predstavljaju veliki rizik po nacionalnu bezbednost.<sup>30</sup>

Koncept nacionalne bezbednosti je rođen iz identifikovanja potrebe za zaštitom od vojnih napada. Međutim, sveprisutna upotreba društvenih medija, nacionalna bezbednost se sada bavi i nevojnim aktivnostima ili dimenzijama.<sup>31</sup> U skladu sa teorijom igara, uvek će postojati motivacija za igranje sistema, a platforme društvenih mreža su omogućile eksploataciju koja može brzo da dosegne velike razmere i predstavlja pretnju po jednu naciju.<sup>32</sup> Sajber terorizam je sveobuhvatni termin koji se koristi za korišćenje računara i interneta sa namerom da se nanese šteta ili šteta. Sajber terorizam se koristi da utiče na i kontroliše javno mnjenje i utiče na politiku vlade da utiče na ponašanje vlade. Sledeće kategorije sajber terorizma mogu biti olakšane i izvršene preko društvenih mreža: propaganda, finansiranje

<sup>27</sup> Hmoud, H., Nofal, M., Yaseen, H., Al-Masaeed, S., & Alfawwaz, B. (2022): The effects of social media attributes on customer purchase intention: The mediation role of brand attitude. *International Journal of Data and Network Science*, 6(4), pp. 1543-1556.

<sup>28</sup> Dwivedi, Y.K., Kelly, G., Janssen, M., Rana, N.P., Slade, E.L. & Clement, M. (2018): Social media: The good, the bad, and the ugly. *Information Systems Frontiers*, 20(3), pp. 419-423.

<sup>29</sup> Yeboah-Ofori, A. (2018): Cyber intelligence and OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics*, 7(1), pp. 87-98.

<sup>30</sup> Soumya, T.R. & Revathy, S. (2018): Survey on threats in online social media. In: *Proceedings of the 2018 International Conference on Communication and Signal Processing*, Chennai, April 2018. New York: IEEE, pp. 0077-0081.

<sup>31</sup> Norri-Sederholm, T., Norvanto, E., Talvitie-Lamberg, K. & Huhtinen, A. (2020): Misinformation and disinformation in social media as the pulse of Finnish national security. In: Moehlecke De Baseggio, E., Schneider, O. and Szvircev Tresch, T. (eds.) *Social media and the armed forces*, *Advanced Sciences and Technologies for Security Applications*. Cham: Springer, pp. 207-225.

<sup>32</sup> Fang, F., Liu, S., Basak, A., Zhu, Q., Kiekintveld, C. D. & Kamhoua, C. A. (2021). Introduction to Game Theory. In: Kamhoua, C.A., Kiekintveld, C.D., Fang, F. and Zhu Q. (eds.) *Game theory and machine learning for cyber security*. Hoboken: Wiley, pp. 21-46.

terorizma, obuka terorizma, planiranje i izvođenje terorističkih napada i sajber napadi.<sup>33</sup> Hibridni rat nije jasno definisan u literaturi. Ipak, podrazumeva se da se sastoji od ratnih aktivnosti koje uključuju mešavinu mnoštva strategija koje koriste tradicionalno ratovanje i taktike sajber ratovanja, često uz korišćenje stranih izbornih intervencija i širenje dezinformacija. Jedna od najčešćih primena hibridnog ratovanja na društvenim mrežama je izazivanje anksioznosti kroz manipulativne narative kako bi mlade ljude naveli da vode rat protiv svojih nacija.<sup>34</sup> Špijunaža se odnosi na prikupljanje tajnih i poverljivih informacija, poznatijih kao obaveštajni podaci, preko izvora i insajdera, bez saglasnosti nosioca informacije. Špijunažu sprovode špijuni, a uobičajene prakse ciljanja u špijunske svrhe bile su lociranje prirodnih resursa, kontrola raspoloženja prema politici, prikupljanje informacija o vojnim sposobnostima i kontraobaveštajne službe.<sup>35</sup> Sajtovi društvenih mreža mogu se koristiti za regrutovanje špijuna i špijunaže. Ovo se radi stvaranjem lažnih naloga, sklapanjem prijateljstava i odnosa sa ciljanim ljudima, poznavanjem njihovih slabosti i pokušajem da ih iskoriste i da ih pretvore u špijune. Špijunaža se odnosi na prikupljanje tajnih i poverljivih informacija, poznatijih kao obaveštajni podaci, preko izvora i insajdera, bez saglasnosti nosioca informacije. Špijuni sprovode špijunažu i uobičajene prakse ciljanja u svrhu špijunaže kako bi locirali prirodne resurse, kontrolisali raspoloženje prema politici, prikupili informacije o vojnim sposobnostima i kontraobaveštajne službe.<sup>36</sup>

Društvene mreže se koriste kao oruđe u rukama ekstremističkih terorističkih organizacija za poljuljanje intelektualnih ubeđenja i širenje subverzivnih ideologija. Ekstremističke i terorističke organizacije koriste sajtove društvenih mreža da regrutuju nove članove, komuniciraju i razmenjuju planove i šire ekstremističku ideologiju.<sup>37</sup> Dezinformacija predstavlja širenje informacija koje se imaju za cilj da obmanu građani neke zemlje.<sup>38</sup> Društvene mreže su glavno sredstvo za kampanje dezinformisanja, pri čemu se lažne informacije daju sa namerom da se obmane. Ako strani protivnik promoviše dezinformacije, to može oslabiti ciljanu zemlju.<sup>39</sup> Glavni problem je to što većini korisnika nedostaju digitalne veštine potrebne da bi svoje komunikacione, poslovne ili zabavne potrebe obavljale u virtuelnom okruženju na bezbedan način, uprkos činjenici da je korišćenje informacionih i komunikacionih tehnologija sve više integrisano u svakodnevni život savremenog čoveka. Posebno je značajna činjenica da deca sve više koriste digitalnu tehnologiju u ranom uzrastu. Međutim, bez od-

<sup>33</sup> Al-Husban, M., Al-Husban, A. & Yaseen, H. (2017): Cyber Attack Detection technique to Improve Cyber Security Using Data Mining Methods. In: Proceedings of the International Cyberpolitics, Cyberlaw and Cybersecurity Conference, Istanbul, May 2017. Istanbul: Siber Political Dergisi.

<sup>34</sup> Fabian, S. (2019): The Russian hybrid warfare strategy: Neither Russian nor strategy. *Defense & Security Analysis*, 35(3), pp. 308–325.

<sup>35</sup> Rivera, R., Pazmiño, L., Becerra, F. & Barriga, J. (2022): An analysis of cyber espionage process. In: Rocha, Á., Fajardo-Toro, C.H. and Rodríguez J.M.R. (eds.) *Developments and advances in defense and security, Smart Innovation, Systems and Technologies*. Singapore: Springer, pp. 3–14.

<sup>36</sup> Ibid

<sup>37</sup> Al-Masaeed, S. (2018): Islamic State E-Caliphate on Twitter: An Observational Study. *Al-Balqa Journal for Research and Studies*, 21(1), 5.

<sup>38</sup> Lukito, J. (2020): Coordinating a multi-platform disinformation campaign: Internet research agency activity on three U.S. social media platforms, 2015 to 2017. *Political Communication*, 37(2), pp. 238–255.

<sup>39</sup> Više o tome: Beskow, D.M. & Carley, K.M. (2019): *Social cybersecurity: an emerging national security requirement*. Pittsburgh: Carnegie Mellon University.



govarajuće digitalne ekspertize i roditeljskog (ili starateljskog) nadzora, deca postaju laka meta beskrupuloznih hakera.<sup>40</sup>

Karasek (Karasek) se bavio obaveštajnim podacima društvenih mreža kao alatom za potrebe imigracije i nacionalne bezbednosti i naglasio potrebu za obaveštajnim podacima otvorenog koda i praćenjem interneta u cilju otkrivanja i sprečavanja terorističkih aktivnosti. Ovaj rezultat ukazuje na to da je mnoštvo ličnih informacija na internetu primenjeno za otkrivanje i sprečavanje terorističkih aktivnosti, što znači da je poboljšao rad policije u sadašnjem vremenu interneta. Ovi dokazi sugerišu da se lični podaci dobijeni putem interneta mogu koristiti za pružanje obaveštajnih podataka u realnom vremenu kada se pojedinci sele iz jedne zemlje u drugu. Na primer, obaveštajni podaci društvenih mreža se mogu koristiti za skrining pojedinaca kojima su potrebne vize, što znači da ima potencijal da otkrije i spreči pretnje nacionalnoj bezbednosti, kao što je sprečavanje pojedinaca da uđu u zemlju kako bi počinili teška krivična dela.<sup>41</sup>

Feng, Li, Ji, Guo i Meng (Feng, Li, Ji, Guo & Meng) sproveli su studiju o zaustavljanju sajber napada u ranoj fazi i pregledali bezbednosne rizike koji predstavljaju korisnike sajtova društvenih mreža. Autori su priznali ulogu društvenih medija u svakodnevnom životu pojedinaca. Kroz procenu rizika koji se predstavljaju za korisnike, bilo je evidentno da sajтови društvenih mreža predisponiraju pojedince na strašne posledice i pretnje napadima. Na primer, napadači mogu da koriste informacije objavljene na platformama društvenih mreža da pokrenu napade na civile. Ovo sugeriše da iako društvene mreže imaju pojačan nadzor, one imaju potencijal da izlože ljude napadima. Kao posledica društvenog inženjeringa, postalo je očigledno da napadači koriste lične informacije da počine zločin i da ostanu neotkriveni. S obzirom da počinioci koriste lične podatke za razna krivična dela, autori predlažu metode kojima se ovaj porok može zaobići, kao što je obezbeđivanje edukativnih programa i obuke pre nego što korisnici društvenih mreža budu napadnuti.<sup>42</sup> Sajber-kriminalci su doprineli smanjenju poverenja korisnika Interneta tako što su zloupotrebljavali njihove podatke, ili aktivnostima koje su fizički i psihički mogle da nanesu ljudima štetu.<sup>43</sup> Autori su predložili upotrebu tehnike procene koja analizira bazu informacija ljudi koji su bili žrtve, gde se lične informacije, kao što su sematske karakteristike i statistički atributi, stavljaju u perspektivu. Krajnji cilj je korišćenje funkcija i sastavljanje ocene bezbednosnog rizika dobijenog iz modela analize korisnika, gde se korisnici društvenih mreža sa višim ocenama bezbednosti upozoravaju na mogući napad.<sup>44</sup> Analiza društvenih mreža igra važnu ulogu u utvrđivanju načina na koji se informacije sa različitih medijskih platformi koriste za različite funkcije za sprečavanje bezbednosnih pretnji. Postoje dokazi koji upućuju na to da većina zemalja nema političke i zakonske okvire koji im omogućavaju da koriste društvene mreže kao alat za bez-

<sup>40</sup> Baltezarević, R. (2022): Digitalna pismenost kao sredstvo prevencije protiv sajber kriminala. *Baština*, Vol. 32 sv. 57, pp. 131-139 DOI: <https://doi.org/10.5937/bastina32-38103>.

<sup>41</sup> Karasek, P. (2018): Social Media Intelligence as a tool for immigration and national security purposes. *Przegląd Bezpieczeństwa Wewnętrznego*, 10(19), 405-415.

<sup>42</sup> Više o tome: Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019): Stopping the cyberattack in the early stage: assessing the security risks of social network users. *Security and Communication Networks*.

<sup>43</sup> Baltezarević, I. & Baltezarević, R. (2021): Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280 UDK 343.533::004 DOI: 10.5937/MegRev2104269B.

<sup>44</sup> Više o tome: Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019): Stopping the cyberattack in the early stage: assessing the security risks of social network users. *Security and Communication Networks*.

bednosne obaveštajne podatke. Da bi se iskoristio snažan pristup analizi društvenih mreže, potrebno je da bezbednosne agencije iskoriste obuku i tehnološke aspekte pošto ovakav nadzor zahteva izgradnju otpornih i održivih sposobnosti koje podržavaju razmenu informacija svetskih bezbednosnih agencija.<sup>45</sup> Krejgin (Cragin) se fokusirao na napade u Parizu i naveo da su se platforme društvenih mreža pojavile kao ključni kanali za širenje informacija i da su takođe bile instrumentalne u pozivanju na društvene promene. Krejgin je sproveo studiju čiji su nalazi pokazali da su se platforme društvenih mreža pojavile kao ključni izvori informacija i sve važniji u uticanju na razumevanje ljudi o terorističkim aktivnostima i njihovim efektima. Široka upotreba pametnih telefona omogućila je ljudima da prijave sumnjive terorističke aktivnosti i da pomno prate posledice terorističkih napada.<sup>46</sup> Velpelj (Whelpley), sa druge strane, je sproveo studiju o efektima društvenih mreža na nacionalnu bezbednost Sjedinjenih Država i tvrdio da novi i šireći fenomen društvenih mreža i njegove sve veće primene imaju mnogo pozitivnih efekata na nacionalnu bezbednost. Mogu se koristiti kao sredstvo upozorenja ili prevencije, u vojnim kampanjama, na primer, u ratu protiv terorizma, i kao institucionalno sredstvo komunikacije.<sup>47</sup>

#### 4. ZAKLJUČAK

Društvene mreže zbog svoje sveprisutnosti i lakoće pristupačnosti imaju sposobnost da direktno i veoma brzo utiču na veliki broj stanovništva. Kompanije, vlade, političke stranke, duhovne vođe, ekstremističke organizacije koriste domet društvenih mreža za propagiranje odgovarajućih poruka koje imaju uticaj na ljudsku populaciju. U tom kontekstu, društvene mreže takođe igraju veoma važnu ulogu u nacionalnoj bezbednosti jedne zemlje i odbrambene organizacije sve više analiziraju ovaj onlajn prostor kako bi otkrile i predvidele moguće opasnosti. Društvene mreže stvaraju ranjivost kada protivnici namerno propagiraju mržnju, obmanjujuće, lažne poruke i dezinformacije. One igraju kontroverznu ulogu u informacionom ratu i mogu se koristiti i kao oruđe za regrutovanje od strane terorista. Opcije za suočavanje sa ovim izazovima su različite i kreću se od regulisanja interneta do ostavljanja društvenih mreža bez ikakve kontrole. Međutim, potrebno je naglasiti i pozitivne efekte društvenih mreža na nacionalnu bezbednost. Mogu se koristiti kao sredstvo kojim se građani blagovremeno upozoravaju na potencijalnu opasnost od vojne intervencije ili terorističkog napada, ili kao efikasno institucionalno sredstvo komunikacije.

#### LITERATURA

- Al-Husban, M., Al-Husban, A. & Yaseen, H. (2017): Cyber Attack Detection technique to Improve Cyber Security Using Data Mining Methods. In: Proceedings of the Inter-

<sup>45</sup> Više o tome: Marcellino, W., Smith, M. L., Paul, C., & Skrabala, L. (2017): Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations. RAND Corporation.

<sup>46</sup> Cragin, R. K. (2017): The Challenge of Foreign Fighter Returnees. *Journal of Contemporary Criminal Justice*, 33(3), 292–312.

<sup>47</sup> Više o tome: Whelpley, T. N. (2014): The effects of social media on US National Security.



- national Cyberpolitics, Cyberlaw and Cybersecurity Conference, Istanbul, May 2017. Istanbul: Siber Political Dergisi.
- Al-Masaeed, S. (2018): Islamic State E-Caliphate on Twitter: An Observational Study. *Al-Balqa Journal for Research and Studies*, 21(1), 5.
  - Baltezarević, I. & Baltezarević, R. (2021): Sajber bezbednost: izgradnja digitalnog poverenja, *Megatrend Revija*, Vol. 18 (4). pp. 269-280 UDK 343.533::004 DOI: 10.5937/MegRev2104269B
  - Baltezarević, R. (2022): Digitalna pismenost kao sredstvo prevencije protiv sajber kriminala. *Baština*, Vol. 32 sv. 57, pp. 131-139 DOI: <https://doi.org/10.5937/bastina32-38103>.
  - Baltezarević, R. & Baltezarevic, I. (2023): Terorizam u digitalnom okruženju. *Baština*, Vol. 33 sv. 60, pp. 173-181 doi: <https://doi.org/10.5937/bastina33-44435>
  - Beskow, D.M. & Carley, K.M. (2019): Social cybersecurity: an emerging national security requirement. Pittsburgh: Carnegie Mellon University.
  - Brown, H. (1983): Thinking about National Security. Boulder, CO: Westview.
  - Buzan, B., Wæver, O. & De Wilde, J. (1998): Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.
  - Buzan, B. & Little, R. (2000): International systems in world history; remaking the study of international relations. Oxford: Oxford University Press.
  - Buzan, B. & Hansen, L. (2009): The evolution of international security studies. New York: Cambridge University Press.
  - Cao, Y., Ajjan, H., Hong, P. & Le, T. (2018): Using social media for competitive business outcomes. *Journal of Advances in Management Research*, 15(2), pp. 211–235.
  - Charles-Philippe, D. (2001): A Guerra e a Paz: Abordagens contemporâneas da Segurança e da Estratégia. Lisbon: Instituto Piaget.
  - Christiansson, M. (2004): Säkerhetspolitisk teori, 1. ed., Stockholm: Militärhögskolan Karlberg.
  - Christensen, T., Lægreid, P. & Rykkja, L.H. (2015): The challenges of coordination in national security management: The case of the terrorist attack in Norway. *International Review of Administrative Sciences*, 81(2), pp. 352–372.
  - Choi, T. M., Guo, S. & Luo, S. (2020): When blockchain meets social- media: Will the result benefit social media analytics for supply chain operations management? *Transportation Research Part E: Logistics and Transportation Review*, 135, 101860.
  - Cragin, R. K. (2017): The Challenge of Foreign Fighter Returnees. *Journal of Contemporary Criminal Justice*, 33(3), 292–312.
  - Dwivedi, Y.K., Kelly, G., Janssen, M., Rana, N.P., Slade, E.L. & Clement, M. (2018): Social media: The good, the bad, and the ugly. *Information Systems Frontiers*, 20(3), pp. 419–423.
  - Fabian, S. (2019): The Russian hybrid warfare strategy: Neither Russian nor strategy. *Defense & Security Analysis*, 35(3), pp. 308–325.
  - Fang, F., Liu, S., Basak, A., Zhu, Q., Kiekintveld, C. D. & Kamhoua, C. A. (2021). Introduction to Game Theory. In: Kamhoua, C.A., Kiekintveld, C.D., Fang, F. and Zhu Q. (eds.) Game theory and machine learning for cyber security. Hoboken: Wiley, pp. 21–46.

- Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019): Stopping the cyberattack in the early stage: assessing the security risks of social network users. *Security and Communication Networks*.
- Guedes, M. & Elias, L. (2010): *Controlos Remotos Dimensões Externas Da Segurança Interna Em Portugal*. Coimbra: Almedina.
- Hmoud, H., Nofal, M., Yaseen, H., Al-Masaeed, S., & Alfawwaz, B. (2022): The effects of social media attributes on customer purchase intention: The mediation role of brand attitude. *International Journal of Data and Network Science*, 6(4), pp. 1543-1556.
- Huang, S.Y. & Ban, T. (2020): Monitoring social media for vulnerability: Threat prediction and topic analysis. In: *Proceedings of the 19th International Conference on Trust, Security and Privacy in Computing and Communications*, Guangzhou, January 2021. New York: IEEE, pp. 1771-1776.
- Jackson-Preece, J. (2011): *Security in international relations*. London: University of London, London School of Economics and Politics.
- Lukito, J. (2020): Coordinating a multi-platform disinformation campaign: Internet research agency activity on three U.S. social media platforms, 2015 to 2017. *Political Communication*, 37(2), pp. 238-255.
- Marcellino, W., Smith, M. L., Paul, C., & Skrabala, L. (2017): *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. RAND Corporation.
- Mention, A.L., Barlatier, P.J., & Josserand, E. (2019): Using social media to leverage and develop dynamic capabilities for innovation. *Technological Forecasting and Social Change*, 144, pp. 242-250.
- Norri-Sederholm, T., Norvanto, E., Talvitie-Lamberg, K. & Huhtinen, A. (2020): Misinformation and disinformation in social media as the pulse of Finnish national security. In: Moehlecke De Baseggio, E., Schneider, O. and Szvircev Tresch, T. (eds.) *Social media and the armed forces*, *Advanced Sciences and Technologies for Security Applications*. Cham: Springer, pp. 207-225.
- Oche, O. (2005): Low Intensity Conflicts, National Security and Democratic Sustenance, in Saliu, H A. (ed.) *Nigeria under Democratic Rule 1999-2003*, Ibadan University, Ibadan.
- Okodolor, C. (2004): National security and foreign policy: towards a review of Nigeria`s afro-centric policy. *Nigerian Forum*, Vol. 25, Nos. 7-8, pp: 204-223
- Olanrewaju, A.S.T., Hossain, M.A., Whiteside, N. & Mercieca, P. (2020): Social media and entrepreneurship research: A literature review. *International Journal of Information Management*, 50, pp. 90-110.
- Onuoha, F. C. (2008): Oil pipeline sabotage in Nigeria: Dimensions, actors and implications for national security. *African Security Review*, Vol.17, No.3, pp. 98-115.
- Pitswane, J. (1993): Recognizing the non-military dimensions of national security: an agenda for the 1990s. *Peace Research*, 25(4):31-38.
- Rivera, R., Pazmiño, L., Becerra, F. & BarrigA, J. (2022): An analysis of cyber espionage process. In: Rocha, Á., Fajardo-Toro, C.H. and Rodríguez J.M.R. (eds.) *Developments and advances in defense and security*, *Smart Innovation, Systems and Technologies*. Singapore: Springer, pp. 3-14.

- Soumya, T.R. & Revathy, S. (2018): Survey on threats in online social media. In: Proceedings of the 2018 International Conference on Communication and Signal Processing, Chennai, April 2018. New York: IEEE, pp. 0077–0081.
- Tha'er Majali, M.A., Omar, A. & Alhassan, I. (2021): Social media use as health awareness tool: A study among healthcare practitioners. *Multicultural Education*, 7(2), pp. 1-5.
- Terrif, T., Croft, S., James, L. & Morgan P.M. (1999): Security studies today. Malden, Massachusetts: Blackwell Publishers incorporated.
- Van Heekeren, M. (2020): The curative effect of social media on fake news: A historical re-evaluation. *Journalism Studies*, 21(3), pp. 306–318.
- Viotti P.R. & Kauppi, M.V. (1999): International relations theory: realism, pluralism, globalism and beyond. Boston: Allyn and Bacon.
- Waever, O. (1995): Securitization and Desecuritization, in Lipschutz, R.(ed.), *On Security*, Columbia University Press, New York, pp. 46-86.
- Whelpley, T. N. (2014): The effects of social media on US National Security.
- Williams, P.D., ed. (2008): Security studies an introduction. New York: Routledge.
- Yeboah-Ofori, A. (2018): Cyber intelligence and OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics*, 7(1), pp. 87–98.

## NATIONAL SECURITY - THE ROLE OF SOCIAL NETWORKS

**Summary:** *Social networks have permeated all spheres of modern society. They enable online connection of users with their friends and family, research of necessary information, entertainment, and online shopping. Social networking sites are increasingly being used by companies to communicate with their target market, and even governments themselves are becoming aware of their utility. However, as a relatively still unsettled area (primarily legally), social networks are a place where the activities of cyber attackers are increasingly taking place, which can threaten both the security of individuals and the state itself. There are more and more examples in which cyber terrorists, using social network sites, spread misinformation, ideology, cause fear, but also recruit their supporters, thereby directly threatening national security. On the other hand, social networks can, at the same time, be a very useful for the protection of national security, as a very effective tool for communication with the population in situations where it is important to quickly warn people about the potential danger of terrorist activity.*

**Keywords:** *Social networks, National security, Cyber attackers, Cyber terrorism*