UDC 327.88::323.28
343.3::004
DOI: 10.5937/spm83-46059
Review paper

Српска политичка мисао
број 1/2024.
Vol. 83
стр. 161-177

Ivana Luknar[*]
Institute for Political Studies, Belgrade

Filip Jovanović[**]
Faculty of Project and Innovation Management, Educons University, Belgrade

VARIOUS TYPES OF CYBER THREATS[***]

Resume

Security of the Internet and online communication has become an essential challenge in contemporary world. Paper discusses different types of cyber threats: cyber-attack, cyber terrorism and cybercrime. Individuals, companies and the states rely their communication and daily functioning on information and communication technologies (ICT). The purpose of the study is to highlight importance of the ICT safety use by pointing to seriousness of the cyber threats. The main methods applied in paper to examine published scientific materials are: inductive and deductive method, analytical and synthesis method, hypothetical-deductive method and method of content analysis. Results of the study indicate need for actively dealing with cyber threats. The intent of this study is both to inform and raise awareness of cyber threats within the communities. Findings of the study contribute to the broader knowledge in research area.

Keywords: cyber threats, cyber-attack, cyber terrorism, cybercrime, cyber security, cyber defence

[*] E-mail address: ivana.luknar@ips.ac.rs.

[**] E-mail address: filip.jovanovic@pmc.edu.rs.

[***] This paper was written within the research activity of the Institute for Political Studies, funded by the Ministry of Science, Technological Development, and Innovation of the Republic of Serbia.

INTRODUCTION

Nowadays world is facing race in development of technology. Such a competitive atmosphere brings numerous challenges to adjust to new technologies as inevitable part of everyday life. „Development of digital technology has produced many benefits to society, but it has also produced a wide range of cyber threats. Those threats can seriously harm and target individuals, industry, critical infrastructures and even governments" (Luknar 2020, 621). Increasingly adopting of ICT and artificial intelligence all around the world, will push question of ICT and AI reliability in the foreground. Since individuals, companies and states increasingly relying on ICT and modern technology innovations, security of ICT and AI becomes more urgent. Given the urgency of addressing these issues, the need for understanding of cyber threats has increased. Analysing different types of cyber threats shows the demands for well-prepared cyber defence both in government and private sector. Cyber threats are developing rapidly along with a technological evolution. It is of great importance to be prepare for further cyber risks. This study proposes actively carry out of expert's research and cooperation, experience exchange and training.

This study presented a wide array of literature related to cyber threats and perceptions of it. The study is structured into eight sections, including the above introduction. Section 2 presents methodology and theories, thereby constructing hypothetical exploratory framework. Section 3 emphasizes the topical importance of the cyber-attack and discusses theory implications about cybercrime and cyber terrorism. Section 4 discusses the AI possibilities in cyber security. Section 5 discusses results of the analysis. Finally, Section 6 concludes this study.

METHODOLOGY AND THEORETICAL FRAMEWORK

Dealing with cyber-attack is important and not easy task. In the current research our main objective is to draw attention to cyber threats and prevent this issue. Consideration of cyber threats can be developed by using theoretical framework presented here. As Zhuge mentioned new methodology to be insightful and predictable should evolved continuously with technology development and "break the boundaries of existing disciplines" (Zhuge 2011, 1014).

Cyber security experiences and trust to the security systems of cyber services is important part of cyber security. Cyber security continuously developing. Exchange of best practices have a crucial role in the cyber defence. By doing this, we aim to provide a clearer description of the possible cyber threats. In this paper we closely examine the existing approaches to address wide range of cyber threats. „Louvain method" may be useful in detection of cyber terrorist groups. The identification of terrorist communities is of crucial importance as they may help to uncover and track their cyber activities. Researchers found that this method was successful to detect "the community structure of large networks" (Blondel et al. 2008, 1) such as cyber space (Croitoru et al. 2015). That is a heuristic method, based on modularity optimization. Social network services and mobile phone networks characterize large size. So, decomposing the networks into sub-units or communities appears as promising approach (Fortunato et al. 2007). Blondel and colleagues (2008) mentioned detection algorithms to distinguish several types of community: „divisive algorithms detect inter-community links and remove them from the network, agglomerative algorithms merge similar nodes/communities recursively and optimization methods are based on the maximization of an objective function" (Blondel et al. 2008, 2).

There were numerous attempts to present a cyber-security framework. Here find enclosed vital theories for the consideration of all kinds of cyber threats. According to that, author suggest „a formal model of the similarity ratio" that „enables aggregation of experiences from many services about the security system of a specific service" (Bahtiyar and Cag˘layan 2013, 290).

According to The Routine Activity Theory mitigation of cyber threats should become routine. Theory suggests "Reducing the opportunities for cybercrime to occur, making cybercrime more difficult to commit and by increasing the risks of detection and punishment associated with committing cybercrime" (Choo 2011, 719). Scholars mentioned "cyber threat modelling" as "an analytical process that is used for identifying the potential threats against a system and supporting the selection of security requirements in the early stages of the system development life cycle" (Mamdouh Khalil et al. 2023).

To understand how science and technology might contribute to countering all types of cyber threats we must evaluate the nature of the threat. There are many approaches to that:

1) human approach – dealing with the cyber-attack from the aspect of the cyber-attacker or cyber user. Weather is cyber-attack individual/personal act or act of a member of a specific organization: terroristic or criminal, the human element is important part of cybersecurity. Researcher of cyber-attacks have noticed the rising number of incidents caused by social engineering (Abraham and Chengalur-Smith 2010; Jansson and Solms 2010). Social engineering malware appear as a major threat nowadays (Mitnick, Simon and Woyniak 2002). Jansson and Solms (2010) presented „a holistic solution in the form of a flowchart" (Jansson and Solms 2010, 24) as guidance that may to help employees 'do the right thing' when they faced with a potential social engineering attack. Researches (Siponen 2000; Luknar 2022) found that each of us play important role in shaping the reliability of ICT. The lack of awareness about cybersecurity policies and best practices has been identified as trigger for malware attack (Siponen 2000);
2) technological approach – dealing with the availability of technical solutions to the vulnerabilities that are most likely to be exploited by cyber-attackers;
3) policy approach – dealing with the vulnerabilities of targets in civil society, examine active cyber policies and strategies;
4) legal approach – dealing with the vulnerabilities of cyber law regulation;
5) consequential approach – dealing with the nature of cyber-attack impacts; the proportions of the cyber-attack damage.

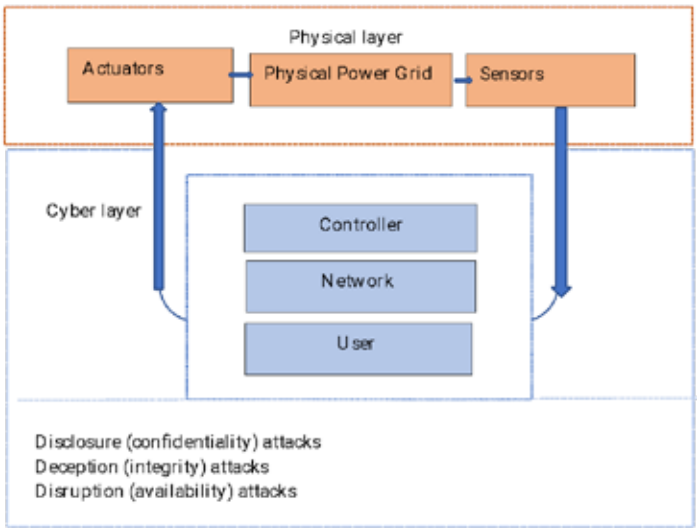
Cyber threat is complex. This concept contains two dimensions: social and technological. Considering the nature of researched issue, combining methods both from technical and social sciences appears as useful solution. Below, we present a summary of scholar works experienced in our own academic work, combined with insights from the research findings of others.

CYBER-ATTACK

Since ICTs have become fundamental tools for contemporary communication, protecting cyber security and preventing cyber-attacks appears as crucial tasks in nowadays world. ICT use haven't changed the goals of communication; however, the methods and techniques continue

to evolve as new ICT means. Trust in ICT depends on the ability to securely communicate. Cyber security main goal is to protect information and cyber service from a wide range of threats. Identifying and classifying threats to information systems is key step to building defensive mechanisms (Luknar 2022). Concurrently, as ICT and cyber defence procedures evolve, cyber threat also evolves. There are so many different kinds of cyber-attacks on cyber-physical systems (CPSs): denial of service (DoS) attacks, bias injection attack, zero dynamics attack, replay attack, stealthy attack, eavesdropping attack, covert attack, dynamic false data injection attacks etc. Cyber-attacks can be classified according to the one or multiple security criteria they are threatening on: "disclosure (confidentiality) attacks, deception (integrity) attacks and disruption (availability) attack" (Canaan et al. 2020, 5). Figure 1 shows connection between physical and cyber layer and three types of cyber-attacks.

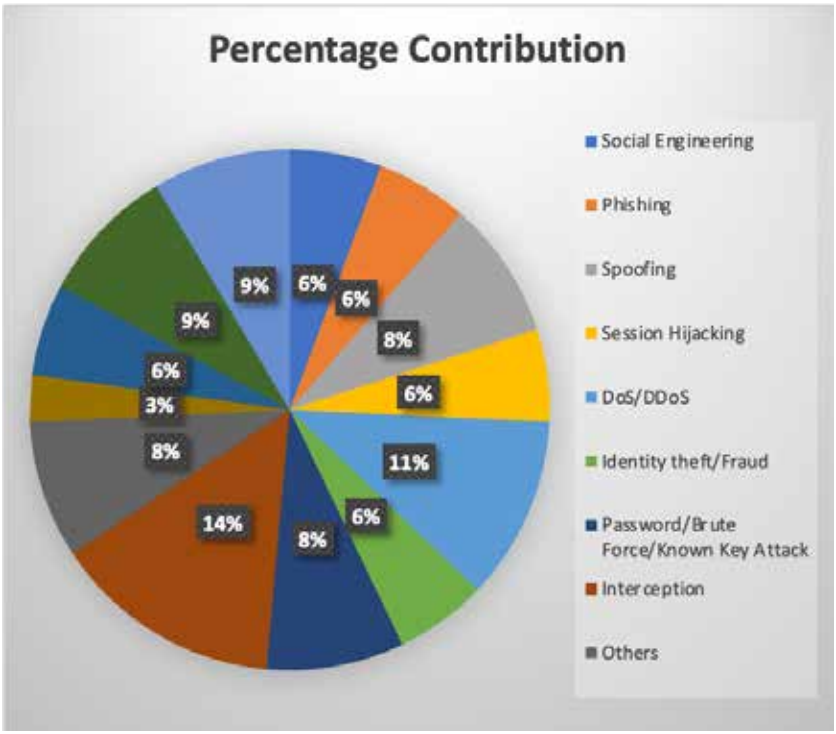
Figure 1.



Source: Canaan et al. 2020, 5.

Cyber-attackers increased the sophistication of their attacks. To deceive a target contemporary cyber-attackers invest time and resources to gather personality traits and other information about their target. Scholars found in their study a percentage of different cyber-attacks in energy sector and trustworthy space, Figure 2 (Priyadarshini et al. 2021).

Figure 2.



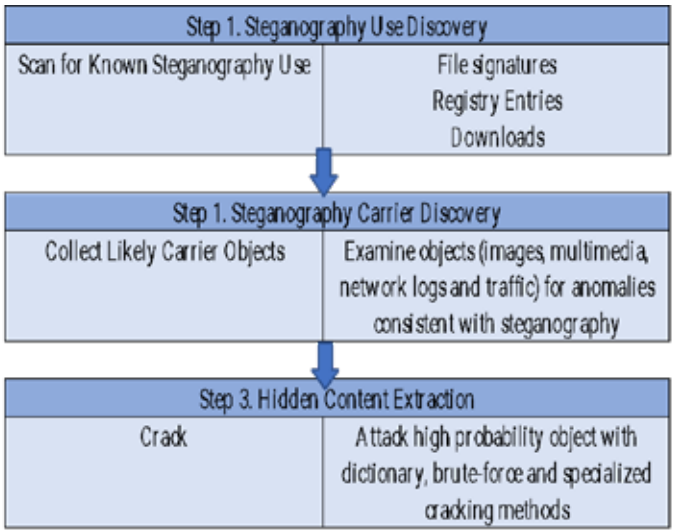
Source: Priyadarshini et al. 2021.

Cyber-attackers use vulnerable entry points to break through the smart grid communication systems. For these interventions they often use the help of numerous mediums, such as the (USB) thumb drive, viruses, and even software patches and updates. People certainly made progress in forensic investigation, although each case and circumstances are different. Different authors have been proposed several cyber-attack detection schemes in recent time. Rago and Hosmer (2013) provided a basic model (Table 1) for uncovering data hiding and steganography activities in three steps:

1) Steganography Use Discovery, refers to actions that requires access to the suspect data storage containers in order to create a forensically sound image of the suspect's data storage devices. That means to examine any actions performed by the suspect that would point to a discovery and examine of all local or remote storage devices, memory sticks, SD Cards, web history, downloaded applications, network searches etc.

2) Steganography Carrier Discovery means three types of analysis of each of the collected object made in previous step: a) "signature-based anomaly detection algorithms"; b) "sophisticated blind steganography detection algorithms", c) human analyst examines manually the results from two previous steps;
3) Hidden Content Extraction – essential ingredient for cracking is discovering the steganography program that was used by the suspect (Rago and Hosmer 2013, 214−215).

Table 1.



Source: Rago and Hosmer 2013, 214.

Authors worldwide propose various methods to detect cyber-attack. Mo et al. propose a computationally-efficient scheme to detect deception attacks on sensors (Mo, Chabukswar and Sinopoli 2014). Fooladivanda and colleagues (2019) propose "dynamic state estimation schemes" (Fooladivanda et al. 2019) that enable us to detect cyber-attacks efficiently, but these solutions do not mitigate all possible adverse effects. These authors demonstrate the effectiveness of secure state estimation method through simulations of the two types of attacks: synchronous generator attacks and inverter-interfaced power supply attacks in three simulated scenarios:

1) Scenario 1: There is no cyber-attack on the microgrid.

2) Scenario 2: The microgrid is under cyber-attack, and it is not protected by any secure state estimation.

3) Scenario 3: The microgrid is under cyber- attack, and it is protected by the proposed secure state estimation (Fooladivanda et al. 2019). Other scholars mentioned "noise filtration" (Basseville and Nikiforov 1993) or "disturbance attenuation techniques" (Jiao et al. 2016) to detect and remove malicious attacks. Diversity of cyber-attacks led to creation of different detection and defense methods and mechanisms. That is why cyber-attackers are developing increasingly complex stealth tactics to avoid progressive forensic procedures and data concealing detection. "Cyber defenses need to be implemented or adapted to keep pace. A key distinction is in the nature of cyber-attackers – they are malicious, persistent, and evolve their attacks over time" (Byrne et al. 2014, 524). Cyber-attack could severely impact states in many different ways. Yue suggested three techniques that each country should be run to achieve the cybersecurity: "optimal design, persistent network vigilance and next-generation security" (Yue 2003, 565–569).

CYBERCRIME

The rapid adoption of ICT created opportunities for crime and deviance online. ICT use dramatically has changed crime. Cybercrime means "crimes that exist simply as a result of the use of the Internet as a means to transmit, access, or share data" (Holt 2016, 31) There are various forms of cybercrime. Many of them are simply electronic parallels of traditional crimes. Cybercrime may involve a wide range of attacks that can be classified in three categories:

1)"crimes specific to the internet";

2)"traditional" crimes such as fraud and forgery committed online;

3)"illegal online content", including pornographic and child sexual abuse material, glorification of violence, terrorism, racism and xenophobia etc. (Luknar 2022, 149).

Henson noticed that "cybercrime victimization is often considered less serious than traditional street crime because of the lack of direct physical contact between the offender and victim" (Henson, Reyns, and Fisher 2016, 567). Studies found that individuals felt emotional upset produced by cybercrime victimization (Symantec 2010). Some types of

cyber victimization were very extreme and may influence mental health (Hinduja and Patchin 2010; Mitchell, Finkelhor, and Becker-Blease 2007). Although a lot has been done regarding this issue, there are still several major limitations that affect our cybercrime defense and knowledge:

- the lack of official data sources that can be use to estimate prevalence or incidence of cybercrime, and may help better to understand the nature of this criminal events.
- the lack of information – People are aware of cybercrime threat. In 2019 the Cyber Barometer from Europe Assistance and LEXIS published results of survey that was conducted in 9 countries (the United States, Italy, France, Spain, Switzerland, Austria, Hungary, Czech Republic, and Romania). 800 consumers from each country, ages 25-75 took part in this survey. Study has found that "46% of consumers are worried about cybercrime. This number rises to 49 percent for respondents with elderly parents and 54 percent for those with children" (Europ Assistance 2019). Other study found that "the general public must become more cognizant of the threat and severity of cybercrimes. There is some evidence that citizens either do not know whom to contact in the event that they experience cybercrimes or think that this experience may not be treated in the same fashion as being the victim of street crime" (Holt 2016, 41).
- cybercrime law – People (criminologists, lawyers, policy makers etc.) have begun to examine ways in which individual utilize technology to engage in crime. The Cybercrime Convention is multinational agreement (Sunde 2018) in which parties must criminalize certain cybercrimes in their national substantive criminal law. Local law enforcement, should be "capable of ensuring that cybercrimes can be properly investigated at all levels of law enforcement" (Holt 2016, 41). "One major issue is that 'traditional' lawyers may not be fully aware of technological developments, whereas technical security experts may not be fully aware of legal issues. This has given rise to a new category of legal advice involving hybrid specialists with legal and technical knowledge, rather than a coordinated team of legal experts working with cyber security experts" (Boobier 2020, 239).

There is a need for the development and assessment of contemporary policy and contra measures against cybercrime. Here are some "recommendations that can be taken to ensure multilevel defense of cybercrime:

1) Consciousness use of the internet;
2) Consciousness implementation of new digital technology
3) International monitoring, juridical cooperation
4) Multilevel transnational cooperation
5) Reducing dark number
6) Law enforcement responses
7) Improve cybercrime policing
8) Dedicated well trained police personnel" (Luknar 2022, 149)

CYBER TERRORISM

Cyber terrorism and cybercrime are two different concepts. Imagine the following scenario: terrorist hacks into a personal bank account to steal funds. This is a case of cybercrime committed by a terrorist, even if the gained money will be used to support terrorism. Although cybercrime and cyber terrorism may seem difficult to divide, cyber terrorist's actions characterize ideological motivation, not pure profit. Cybercriminals intent to satisfy their personal needs and desires. Criminal violence is often opportunistic. Cyber terrorist's aim is to achieve a political, social, or religious change. Cyber terrorist's activities imply fatal level of distraction so they can send certain political message or produce fear on a larger scale. Terrorist are motivated by the future outcomes of their acts. They see present and past as opposite of their aims. "Terrorists now have the unprecedented ability to disrupt our lives, hold information hostage, and/or cause widescale damage by attacking just a few non-human targets that comprise single points of failure within our technology infrastructures" (Rogers 2003, 90). To discuss cyber terrorism, it is necessary to understand the attraction of cyberspace for the terrorist, and the nature of traditional terrorism. The motivation for cyber terrorism attack is the same as for the traditional terrorism. Studies have found different motivation for becoming terrorist. It seems to vary as much as the personalities of the terrorists themselves (Rogers 2003; Reich 1990).

Rogers (2003) defines cyber terrorist as "individual who uses computer/network technology to control, dominate or coerce through the use of terror in furtherance of political or social objectives" (Rogers 2003, 78). "The targets selected by terrorists will depend on their goals, but the choice of attacks will depend on five important criteria: opportunity to

(a) Inflict loss of human life in large numbers,

(b) Destroy important physical facilities,

(c) Exact severe economic damage for a persisting period of time,

(d) Disrupt the institutions of government, and

(e) Attack symbols of civil culture most detested by the terrorists" (Branscomb 2004, 274). Bennet (2017) mentioned some of the objectives of terrorism:

- "Demonstrate the group's power over the population and government;
- Show the existing government's lack of power to interfere or stop terrorist operations.
- Exact revenge for perceived persecution and satisfy the group's vengeance.

Gain worldwide, national, or local publicity for the group's cause by attracting media coverage" (Bennet 2017, 9). Cyber-attack may couse various kinds of effects like misinformation, degradation of GPS, confusion, displaying private data etc. (Yannakogeorgos 2012) .

Confronting cyber terrorism requires readiness and vigilance at all time, despite the apparent absence of visible terrorist activity. "To understand how science and technology might contribute to countering terrorism, one must evaluate the nature of the threat, the vulnerabilities of targets in civil society, and the availability of technical solutions to the vulnerabilities that are most likely to be exploited by terrorists" (Branscomb 2004, 272).

ARTIFICIAL INTELLIGENCE

Artificial intelligence has engendered a great deal of excitement and controversy. Our fascination with AI runs deeper than fear. The allure of AI is unquestionable. Worldwide AI debate is based on two issues. First issue is connected with its widespread use in a nowadays world without adequate law frame. It concerns the consequences. Second issue is about AI limitations. With risk and consequence, arises question of substantive AI ethic. Its ethical principles are matter of reflections and speculation. That is why some authors see AI as threat. "AI is also leading to a whole new generation of autonomous weapons and countless variants of extremely dangerous cyber-attack tactics, including "deep fakes". This of

course does not mean that AI is evil per se, but that humans could rely on AI to realize both virtuous and malicious goals, including building more deadly weapons and breaking security walls" (Renda 2019, 5).

AI algorithms showed incredible possibilities. AI has already applied in various sectors such as: digital platforms, defense, cyber security, e-banking, healthcare, energy, insurance, e-commerce etc. We have the chance to make AI policy choices and application of AI algorithms in a best possible way to improve cyber security from various cyber threats. Recommendation is to integrally connected AI algorithms to the concept of cyber threat. While different simulations can be used for cyber defense trainings and education about diverse cyber threats. As Renda noticed "new risks will also emerge" (Renda 2019, 22). So, governments should consider "the restructuring of cyber security and cyber-resilience plans, with the creation of pervasive, diffuse networks of data collection points, coupled with the centralization of processing power into high performance computers" (Renda 2019, 22).

DISCUSSION

With all the innovations in information and communication technology it is clearly accurate that contemporary states in general have become more dependent on network infrastructure. It is necessary for governments to take preventative actions towards all kinds of cyber threats. Governments should consider all infrastructures that rely on technology to run effective cyber defense. Each technological components of the infrastructures must be analyzed to reach high level of preparedness against cyber vulnerabilities. Economically undeveloped countries can't financially afford the high-tech devices, but should consider every possibility to protect critical infrastructures. Cyber-attacker knows no boundaries. As studies have shown in the last few years, a lot has been done on the cyber security issue. Despite, there is a problem with the longevity of high – tech protection. Humans can very well miss out to provide effective cyber security if they don't continuously follow the trends of technological innovations. Stay in touch with newest forms of technology possibilities is prerequisite for dealing with this issue. Monitoring and evaluation of developed cyber security framework worldwide, provides opportunities to improve on time cyber defense. It is necessary to consider all possibilities of artificial intelligence in dealing with cyber threats. The quality of our cyber security depends on the quality

of our approach to cyber threats. A multidisciplinary approach appears as desirable, as cyber threats arise from actions made in complex cyber-physical space. Study highlighted importance of combining methods both from technical and social sciences. Future research directions should also propose different methods in dealing with cyber threats.

CONCLUSION

We have witnessed a significant growth in the use of ICT and artificial intelligence. Covid-19 pushed information and communication technologies to become dominant means of interacting and collaborating. The intersection of the physical and cyber spaces creates new complex virtual spaces for collaboration and interaction. Gaining a better understanding of different kinds of cyber threats is a substantial scientific challenge that may improve our ability to better response to cyber threats. Cyber-attack could produce considerably different consequences, threatening people activities and life. Despite many efforts that have been made to find solutions to cyber security problems, contemporary defense and cyber policies deals with what was done in past. Achieve efficient cybersecurity is not easy. Only, continuous cooperation and tracking trends in technology development may lead to good prevention of various cyber threats.

REFERENCE

Abraham, Sherly, and InduShobha Chengalur-Smith. 2010. "An overview of social engineering malware: trends, tactics, and implications." *Technology in Society* 32: 183–196.

Bahtiyar, Serif, and U. Mehmet Cag˘layan. 2013. "Security similarity-based trust in cyber space." *Knowledge-Based Systems* 52: 290–301.

Basseville, Michele, and Igor Nikiforov V. 1993. *Detection of abrupt changes: theory and application*. New Jersey: Prentice Hall Englewood Cliffs.

Bennet, T. Brian. 2017. *Understanding, Assessing, and Responding to Terrorism. Protecting Critical Infrastructure and Personnel.* New Jersey: Wiley.

Blondel, D. Vincent, Guillaume, Jean-Loup, Lambiotte, Renaud, and Etienne Lefebvre. 2008. "Fast unfolding of communities in large networks." *Journal of Statistical Mechanics: Theory and Experiment* 10. doi: http://dx.doi.org/10.1088/1742-5468/2008/10/P10008.

Boobier. Tony. 2020. *AI and the Future of Banking*. New Jersey: John Wiley & Sons Ltd.

Branscomb, Lewis. 2004. "Protecting civil society from terrorism: the search for a sustainable strategy." *Technology in Society* 26: 271–285.

Byrne DJ, Morgan, David, Tan, Kymie, Johnson, Bryan, and Chris Dorros. 2014. "Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations." *Procedia Computer Science* 28: 522 – 530.

Canaan, Bushra, Colicchio, Bruno, and Dj. Ould Abdeslam. 2020. "Microgrid Cyber-Security: Review and Challenges toward Resilience." *Sustainability* 2020: 5649.

Choo, R., Kim-Kwang, 2011. "The cyber threat landscape: Challenges and future research directions." *Computers & Security* 30 (8): 719–731.

Croitoru, Arie, Wayant, N.; Crooks, A.; Radzikowski J.; Stefanidis, A. 2015. "Linking cyber and physical spaces through community detection and clustering in social media feeds." *Computers, Environment and Urban Systems* 53: 47–64.

Europ Assistance. 2019. "Nearly Half of consumers concerned about cyber risks." 13.2.2019. https://webcache.googleusercontent.com/search?q=-cache:H9xV_7j85VoJ:https://www.europ-assistance.com/wp-content/uploads/2021/02/1549968385135.pdf&cd=1&hl=sr&ct=clnk&gl=rs.

Fooladivanda, Dariush, Hu, Qie, Chang, H. Young, and W. Peter Sauer. 2019. "Secure State Estimation and Control for Cyber Security of AC Microgirds." *arXiv* 2019, arXiv:1908.05843. https://arxiv.org/abs/1908.05843

Fortunato, S.; Castellano, C. 2007. "Community Structure in Graphs." In *Chapter of Springer's Encyclopedia of Complexity and System Science*, ed. Robert Meyers, 1141–1163. New York, NY: Springer. https://doi.org/10.1007/978-0-387-30440-3_76.

Henson, Billy, Reyns, W. Bratfors, and S. Bonnie Fisher. 2016. "Cybercrime Victimization." In *The Wiley Handbook on the Psychology of Violence*, eds. Carlos A. Cuevas, Callie Marie Rennison, 554–570. Hoboken, New Jersey: John Wiley & Sons Ltd.

Hinduja, Sameer, and Justin Patchin W. 2010. "Bullying, cyberbullying, and suicide." *Archives of Suicide Research* 14: 206–221.

Holt, J. Thomas. 2016. "Cybercrime." In *The Handbook of Measurement Issues in Criminology and Criminal Justice*, eds. Beth M. Huebner, Timothy S. Bynum, 29–48. New Jersey: John Wiley & Sons Ltd.

Jansson, Kenny Olof Robert, and Solms von Rossouw 2010. "Social Engineering: Towards A Holistic Solution." In *Human Aspects of Information Security Assurance*. Proceedings of the South African Information Security Multi-Conference (SAISMC), eds. Nathan Clarke, Steven Furnell, Rossouw von Solms, 23–34. South Africa: Port Elizabeth.

Jiao, Qiang, Modares, Hamidreza, Lewis, L. Frank, Xu, Shengyuan, and Lihua Xie. 2016. "Distributed α2-gain output-feedback control of homogeneous and heterogeneous systems." *Automatica* 71: 361–368.

Luknar, Ivana. 2020. "Cybercrime – Emerging Issue." In *Archibald Reiss Days*, ur. Stevo Jaćimovski, 621– 628. Beograd: Kriminalističko-policijski univerzitet.

Luknar, Ivana. 2022. "Social control theory and cybercrime." *Nacionalni interes* 41(1): 147–159. doi: https:doi.org//10.22182/ni.4112022.7.

Mamdouh Khalil, S., Bahsi, H., Ochieng' Dola, H., Korõtko, T., McLaughlin, K., and Kotka, V. 2023. "Threat Modeling of Cyber-Physical Systems – A Case Study of a Microgrid System." *Computers & Security* 124: 102950.

Mitchell, J. Kimberly, Finkelhor David, and A. Kathyn Becker-Blease. 2007. "Linking youth internet and conventional problems: Findings from a clinical perspective." *Journal of Aggression, Maltreatment and Trauma.* 15: 39–58.

Mitnick D. Kevin, Simon L. William, and Steve Wozniak. 2002. *The art of deception: controlling the human element of security.* Hoboken, New Jersey: Wiley & Sons.

Mo, Yilin, Chabukswar, Rohan, and Bruno Sinopoli. 2014. "Detecting integrity attacks on SCADA systems." *IEEE Transactions* on *Control* Systems *Technology* 22 (4): 1396–1407.

Priyadarshini, Ishaani, Kumar, Raghvendra, Sharma, Rohit, Kumar Singh, Pradeep, and C. Suresh Satapathy. 2021. "Identifying cyber insecurities in trustworthy space and energy sector for smart grids." *Computers and Electrical Engineering* 93: 107–204.

Rago, M., and Chet Hosmer. 2013. *Data hiding.* Amsterdam, The Netherlands: Elsevier/Syngress.

Reich, Walter. 1990. "Understanding terrorist behaviour: the limits and opportunities of psychological inquiry." In *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed. Walter Reich, 261–280. New York: Cambridge University Press.

Renda, Andrea. 2019. *Artificial Intelligence. Ethics, governance and policy challenges*. Brussels: Centre for European Policy Studies (CEPS).

Rogers, Marc. 2003. "The Psychology of Cyber-terrorism." In *Terrorists, Victims, and Society: Psychological Perspectives on Terrorism and Its Consequences*; ed. Andrew Silke, 77–92. Chichester: Wiley.

Siponen, T. Mikko 2000. "A conceptual foundation for organizational IS security awareness." *Information Management & Computer Security* 8: 31–4.

Sunde, Marie Inger. 2018. "Cybercrime Law." In *Digital Forensics*, ed. Andre, Arnes, 51–116. Hoboken, New Jersey: John Wiley & Sons Ltd.

Symantec. 2010. "*Norton cybercrime report: The human impact* Reveals Global Cybercrime Epidemic and Our Hidden Hypocrisy*."* 8 September 2010. *https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-report-human-impact-reveals-global-cybercrime*.

Yannakogeorgos, A. Panayotis. "The Newest Security Threat: Cyber-Conflict". In *Local Planning for Terror and Disaster: From Bioterrorism to Earthquakes*; Cole, A. L., Connell, D. N., Ed.; Wiley Blackwell 2012, pp. 227–238.

Yue, On-Ching. 2003. "Cyber security." *Technology in Society* 25: 565–569.

Zhuge, Hai. 2011. "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology." *Artificial Intelligence* 175: 988–1019.

Luknar, Ivana. 2022. Sajber terorizam: mere za suzbijanje i prevencija, Beograd: Institut za političke studije.

Ивана Лукнар*

Институт за политичке студије, Београд

Филип Јовановић**

Факултет за пројектни и иновациони менаџмент,
Едуконс универзитет, Београд

РАЗЛИЧИТЕ ВРСТЕ САЈБЕР ПРЕТЊИ

Сажетак

Безбедност интернета и онлајн комуникација постали су један од суштинских изазова садашњице. У раду се разматрају различите врсте сајбер претњи као што су: сајбер напад, сајбер тероризам и сајбер криминал. Појединци, компаније и државе се готово свакодневно у свом раду и комуникацији ослањају на функционисање информационо-комуникационих технологија (ИКТ). Сврха студије је да се укаже на значај безбедности информационо-комуникационих технологија, указивањем на различите врсте сајбер претњи које могу да настану услед примене ИКТ и да изазову озбиљне последице. Приликом истраживања научне грађе на поменуту тему примењене су различите методе: индуктивна и дедуктивна метода, аналитичко-синтетичка метода, хипотетичко-дедуктивни метод и метода анализе садржаја. Резултати студије указују на потребу за континуираним и активним праћењем свих врста сајбер претњи. Намера ове студије је да информише јавност поводом овог проблема и подигне свест о евентуалним сајбер претњама унутар друштва. Налази студије доприносе проширивању знања у овој области истраживања.

Кључне речи: сајбер претње, сајбер напад, сајбер тероризам, сајбер криминал, сајбер безбедност, сајбер одбрана

* Имејл-адреса: ivana.luknar@ips.ac.rs.

** Имејл-адреса: filip.jovanovic@pmc.edu.rs.

* Овај рад је примљен 18. августа 2023. године, а прихваћен на састанку Редакције 06. фебруара 2024. године.