Journal of Digital Law and Policy
Volume 3 Number 1, September 2023
e-ISSN 2808-3458 p-ISSN 2808-3652
https://ejournal.sidyanusa.org/index.php/jdlp

Cybercrime and Threats to the Electoral System

Ni Komang Triana Andini[1], Ni Made Ayu Nadia Putri Damayanti[2], Ni Kadek Wintan Purnama Sari[3], Egidius Fkun[4], Moh. Erkamim[5]

[1,2,3]Institut Bisnis dan Teknologi Indonesia, Denpasar, Indonesia
[4]Prodi Ilmu Pemerintahan, Universitas Timor, Kupang, Indonesia
[5]Universitas Tunas Pembangunan, Surakarta, Indonesia

Email: [1]komangtriana882004@gmail.com, [2]made.ayunadia.Putri@gmail.com,[3]wintanpurnama7@gmail.com, [4]egifkun6@gmail.com,[5]author@lecture.utp.ac.id

Received on *10 07 2023*	*Revised on* *30 08 2023*	*Accepted on* *15 09 2023*

Abstract

Cyberattacks have emerged as a growing threat in the context of elections worldwide, posing significant risks to the integrity, security, and trustworthiness of electoral systems in today's digital age where information technology plays a pivotal role. Drawing from documented cyberattack cases and security reports from government agencies and related organizations during elections, common attack types such as Denial-of-Service (DoS), Phishing, and Malware have been identified. Cybersecurity systems and data sovereignty form the bedrock of personal data protection. As technology advances, data has become a highly valuable commodity, and a nation's data sovereignty intersects with the private sector on a global scale in political and economic terms. The state's primary responsibility lies in crafting regulations for data protection and cybersecurity, ensuring citizens' rights to personal data protection, which necessitates enhancing their capacity and capabilities. Therefore, this qualitative research delves into the imperative of developing citizens' capacity and capabilities in building cybersecurity and data sovereignty, with a particular focus on safeguarding personal data in the Indonesian context, as books and journal articles serve as valuable sources for data collection. Bolstering citizens' capacity and capabilities is essential for preserving their personal data in the digital realm.
Keywords: *cyberattacks, electronic election, election system.*

INTRODUCTION

In the era of globalization, accelerated by information technology, we witness a profound impact on the flow of information and communication, transcending spatial and temporal boundaries. Globalization gives rise to an integrated global community, shaped by two dimensions: spatial and temporal. Spatially, the world becomes more interconnected, while temporally, it contracts. Jan Aart Scholte defines globalization as a process of transforming the global environment, characterized by technological and informational advancement, fostering interdependence and blurring national borders.[1] Thus, these definitions are further expedited by the progress in information technology, resulting in significant and far-reaching consequences in international relations, free from space and time constraints.

Considering the impacts of information technology, many countries perceive it as an opportunity that can contribute positively to their societal and global well-being.[2] However, there are also concerns about it posing an asymmetric threat to their existence. Cyberspace, as a domain where information is stored, shared, and communicated online, is a product of information technology development and represents the latest frontier in fifth-generation warfare, alongside land, sea, air, and outer space. As a new domain, cyberspace interconnects various computerized systems through networks that support critical national infrastructure, forming the core of a nation's life. Despite the efficiency and effectiveness offered by the cyber realm, it has led to convergence and dependency among many nations, experiencing significant escalation year by year. This, in turn, opens the door to high-risk threats to national security. This is why cyberspace has become an arena for asymmetric warfare, vulnerable to a wide range of threats originating not only from internal or external actors but also from individuals, non-state groups, and even nations seeking personal or group benefits, whether monetary, military, or strategic.

General elections, a cornerstone of democracy, are essential but vulnerable to disruption. Political unrest, domestic security instability, and even national defense threats might result from such disturbances. The electoral system, vital to democracy, has attracted cybercriminals. Technology keeps evolving, thus elections increasingly use electronic systems. This technological innovation also adds cybercrimes, which could undermine the democratic process's integrity and trust. Security professionals, the public, governments, and the world are concerned about cybercrime and electoral system assaults. This introduction covers the history, problem statement, research objectives, and expected benefits of the study.

The Indonesian General Election Commission (KPU) uses ICT through the Electronic-Based Government System to organize elections. Regulation No. 5 of 2022 defines this endeavor to improve KPU electronic public services' quality and accessibility. However, the KPU confronts many issues. First, cybercrime exploits every vulnerability in the ever-changing ICT world. Second, digital inequities in Indonesia hinder ICT adoption and security. The KPU has also been targeted by cyberattacks, which have increased in number and severity, making cybersecurity difficult. The KPU needs a robust infrastructure to support its operations due to the wide range of cyber threats and rapid technological innovation. These flaws have been addressed through collaborating with other agencies, as cybersecurity cannot be achieved alone. Indonesia has adopted Cybersecurity 2.0, a collaborative strategy between government, IT, and academic organizations to shape cybersecurity technology. This multimodal approach mitigates vulnerabilities throughout the electoral process to ensure election security and integrity.[3]

[1] Natasha Tusikov Blayne Haggart, Jan Aart Scholte, *Power and Authority in Internet Governance: Return of the State?* (New York: Taylor & Francis, 2021).

[2] Nyoman Amie Sandrawati, “Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan TIK Di KPU,” *Electoral Governance Jurnal Tata Kelola Pemilu Indonesia* 3, no. 2 (2022): 232–57.

[3] Miko Aditiya Suharto and Maria Novita Apriyani, “Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional,” *Risalah Hukum* 17 (2021): 98–107, https://doi.org/10.30872/risalah.v17i2.705.

METHODS

Data security and encryption are key to personal data protection. Technology development makes data a valuable commodity. In economic policy, a nation's data is compared to its worldwide sector. The government's role is to regulate data protection and security. Personal data protection is a national right that requires national capacity and ability. State-centered planning is often used to build cyber security. However, without a people-centered approach, it will be difficult to protect and protect citizens' valuable personal data. This research will examine how building national capacity and capability is necessary for building shareholder security and personal data protection in Indonesia. The author uses a quantitative research method[4] to simplify data collection from books, journal articles, news, and other sources.[5] Research shows that state-centered nation-state dominance in financial security does not guarantee national data security or personal data protection for all citizens. Building citizen capacity and capability is crucial to protecting personal data in the cloud.

RESULT AND DISCUSSION

Over the past few years, cyberattacks on voting systems have increased significantly in many countries. Hacking, malware, and data manipulation can seriously damage public trust in politics. Thus, understanding existing knowledge and identifying potential threats to reduce cyber risk on the chosen system is crucial. The primary objective of this study is to investigate several fundamental inquiries. These inquiries include the classification of different forms of cyberattacks, an analysis of cyberattacks specifically targeting procurement systems, an exploration of the varied responses implemented by different nations to counter these threats, and an examination of the factors that influence the level of cybersecurity in these systems. The primary objective of this research is fourfold: firstly, to conduct a comprehensive analysis of the numerous cyberattacks targeting national systems in different countries; secondly, to clarify the consequences of these attacks on the fundamental principles of integrity and trust that support political decision-making processes; thirdly, to outline the varied responses adopted by nations when faced with cyber threats against their systems; and fourthly, to examine the factors that significantly influence the level of cybersecurity measures implemented for these systems.

The research aims to generate many substantial advantages. The primary objective of this initiative is to increase awareness surrounding the pervasive cyber dangers that procurement systems encounter. Through this endeavor, the aim is to provide knowledge and awareness to both the wider population and governmental entities regarding the extensive ramifications of cyberattacks on political integrity. Furthermore, the research aims to provide useful insights into the development of successful tactics for responding to cyber threats that are specifically customized to the selected systems. Moreover, the objective of this study is to ascertain

[4] H Snyder, “Literature Review as a Research Methodology: An Overview and Guidelines,” *Journal of Business Research*, 2019, 333–39, https://doi.org/https://doi.org/10.1016/j.jbusres.2019.07.039.

[5] Soerjono Soekanto, *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: PT Rajawali Pers, 2015).

essential variables that necessitate consideration during the evaluation of cybersecurity vulnerabilities linked to these systems. The primary objective of this research is to improve cybersecurity protocols and safeguard the integrity of national systems through a thorough examination of cyberattacks.

Types of Cyber Attacks

1) Computer Network Attacks (CNA) are hostile actions or planned acts that alter, disrupt, deny, degrade, or destroy computer and network data or the machines and networks themselves. Organizations have defined cyberattacks differently. Cyberattacks are attempts to disable computers, steal data, or use a hacked computer system to launch more attacks, according to Unisys. IBM describes cyberattacks as unauthorized access to computer systems to steal, expose, change, disable, or destroy information. Cisco Systems, an American networking system business, defines cyberattacks as aggressive and purposeful attempts by individuals or organizations to access others' information systems, frequently for profit.

   Equipment, computer networks, or computer code with destructive characteristics are used to intentionally and unlawfully modify, disrupt, deny access, reduce performance, or damage computer files, networks, or computers. When related to an individual's computer technology rights, cyberattacks that alter, disrupt, deny access, reduce performance, or damage computer files, networks, or computers are clearly uncomfortable and threatening. Threats to information operations include any disruptive element that compromises confidentiality, integrity, and availability. Cyberattacks, natural disasters, and purposeful physical assaults are threats

2) Cyber Attacks in Cyber Crimes: The US Department of Justice defines computer crime as "... any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution." The Organization of European Community Development defines it as "any illegal, unethical, or unauthorized behavior related to the automatic processing and/or transmission of data." Cybercrime, according to Indra Safitri, involves the infinite use of information technology and relies on high-level security and the legitimacy of internet users' information. From these perspectives, cybercrime includes:[6]

   - Computer and network crimes include virus, exploit attacks, and denial of service.
   - Criminals utilize computers or computer networks for identity theft, fraud, cyberstalking, and phishing.

   The Budapest Convention against Cybercrime was signed by 30 nations on November 23, 2001.[7] This convention promotes multilateral cooperation to combat internet and computer network crime. This initiative is intended to inspire international cooperation against high-tech crimes.

3) The Tallinn Manual, designed to address legal gaps in cyber warfare, defines cyberattacks in Rule 30 as offensive or defensive cyber actions reasonably likely to cause injury, death, or property damage. Derived from Article 49(1) of the Geneva Conventions' Additional Protocol I, it underscores that cyber warfare is coordinated with traditional military conflict. Cyber warfare involves entities such as organizations,

[6] Shinta Nurul, Shynta Anggrainy, and Siska Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)," *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)* Vol. 3, no. No. 5 (2022): 564–73.

[7] Jonathan Clough, "A WORLD OF DIFFERENCE: THE BUDAPEST CONVENTION ON CYBERCRIME AND THE CHALLENGES OF HARMONISATION," *Monash University Law Review* 40, no. 3 (2014): 698, http://classic.austlii.edu.au/au/journals/MonashULawRw/2014/28.pdf.

enterprises, and the military targeting other nations' computer networks. Tallinn Manual Rule 41 distinguishes 'means of cyber warfare' as cyber weapons and systems and 'methods of cyber warfare' as tactics, strategies, and procedures. Combatant status is associated with those meeting specified criteria, but cybercrime entails individuals or entities lacking the complex structure required for combatant status and involving subjects and objects that don't qualify. Notably, cyber warfare and cybercrime are governed by distinct international legal frameworks—the Tallinn Manual for cyber warfare and the Budapest Convention on Cybercrime for cybercrime, even among non-ratifying nations.

Types of Cyber Attacks that Often Occur On Election Systems

The initial cyber danger under consideration is the Denial of Service (DoS) Attack. This particular attack aims to disrupt or permanently incapacitate the services provided by a website or application. It achieves this by inundating the server with a multitude of simultaneous requests, utilizing a botnet. The server experiences an excessive influx of request traffic, leading to its unavailability for users and potentially resulting in financial or operational setbacks. Instances such as the assault on the Kaskus website perpetrated by the YogyaFree community serve as illustrative cases that underscore the potential consequences of server security flaws in precipitating such menacing incidents.[8] Mitigation options encompass the utilization of cryptographic hashing, server responses, and the implementation of Snort with predefined rules to effectively limit the influx of inbound ICMP signals.

The second cyber hazard is to the illicit acquisition of personal data and information via the internet, frequently attributable to inadequate regulations governing data protection. According to the International Telecommunication Union (ITU), the release of The Global Cybersecurity Index (GCI) 2017 has classified Indonesia as possessing inadequate cybersecurity measures, therefore emphasizing the imperative for more robust regulatory frameworks.[9] Cybercriminals endeavor to exploit these vulnerabilities for their own benefit, frequently by disseminating deceptive information to increase traffic to websites or by directly pilfering personal data. Prominent instances involving Facebook, such as the Cambridge Analytica incident, have brought to light the susceptibility of user data. Mitigation strategies encompass the reinforcement of data protection legislation and the promotion of international collaboration in the realm of cybersecurity.

One of the cyber threats that is addressed is the rise of counterfeit websites and phishing attempts. Phishing entails the manipulation of website or application content with the intention of deceiving consumers and extracting their personal information. The utilization of such information by cybercriminals serves illicit objectives, hence potentially resulting in unauthorized entry into accounts and subsequent financial detriment. Mitigation tactics encompass several measures, such as the verification of email sender identities, the avoidance of suspicious links, the assurance of secure online connections, and the verification of website domains to ascertain their legitimacy. In summary, there has been a notable rise in cyber threats between 2019

[8] Kaskus, "Serangan DoS Pada Situs Kaskus Oleh Komunitas YogyaFree," 2016, https://www.kaskus.co.id/thread/56c2c8d69a09515e5e8b4567/serangan-dos-pada-situs-kaskus-oleh-komunitas-yogyafree.

[9] International Telecommunication Union, "Global Cybersecurity Index (GCI) 2017" (Geneva, 2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

and 2021.[10] This escalation can be attributed to various variables, including profit-driven goals, vulnerabilities in server security, and heightened levels of online engagement. Preventive measures encompass the reinforcement of legislative frameworks, the facilitation of cybersecurity collaboration, and the promotion of conscientious conduct in the online realm.[11]

How Have Different Countries Responded to These Attacks?

The issue of combating cybercrime is a multifaceted and intricate problem for law enforcement organizations operating within the jurisdiction of Indonesia. Despite the rising prevalence of cyberattacks, the endeavors to effectively implement legal measures against individuals involved in cybercriminal activities continue to exhibit inadequacies. One of the primary hurdles lies in the elusive characteristics of cybercrimes, which frequently pose difficulties in their traceability, as well as the obstacles encountered in the collection of considerable evidentiary support. The insufficiency of legal frameworks governing cybercrime is a prominent issue within the realm of law enforcement endeavors in this domain.

In contrast, elections and concurrent voting play essential roles in the execution of democratic processes. The task of enhancing democracy encounters heightened difficulties in the presence of underdeveloped social, economic, political, and legal circumstances. Hence, it is imperative for the General Election Commission (KPU) to possess a comprehensive understanding of the pertinent legislative frameworks pertaining to cybercrime. This comprehension will not only aid in deterring cybercriminals but also function as a valuable educational resource for preventing comparable attempts in subsequent instances.[12]

Indonesia currently lacks dedicated legislation pertaining to cybersecurity; nonetheless, some existing laws have addressed various facets associated with the deterrence of cybercrimes. The examples provided encompass several laws that pertain to various aspects of governance. These laws are specifically identified as Law Number 36 of 1999, which pertains to Telecommunications, Law Number 19 of 2002, which pertains to Copyright, Law Number 15 of 2003, which pertains to Counterterrorism, and Law Number 11 of 2008, which pertains to Electronic Information and Transactions. Nevertheless, it is vital to get a comprehensive and precise comprehension of cyber regulations.

In order to mitigate the risks posed by cybercrime and address the issue of digital inequities, the KPU has devised proactive strategies aimed at bolstering cybersecurity. The KPU's Decision No. 12 of 2022 demonstrates its dedication to addressing this issue, since it outlines a thorough strategy for enhancing security measures. As a result, the KPU endeavors to uphold the integrity of elections and concurrent voting while implementing measures to protect its systems from any cyber risks.[13]

[10] National Center for Education Statistics, “Protecting Your System: Information Security,” 2023, https://nces.ed.gov/pubs98/safetech/chapter6.asp.

[11] Hino Samuel Jose, “Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 Di Forum Multilateral,” *Populika* 9, no. 2 (2021): 70–85, https://doi.org/10.37631/populika.v9i2.390.

[12] M Syadli Pratama, Fetri Miftach, and Yusuf Ali, “The Cyber Security Strategy of General Elections Commission in Facing the General Election 2019,” *Jurnal Prodi Perang Asimetris* 4, no. 3 (2018): 77–94.

[13] Sahat Parulian, Devi Anassalifa Pratiwi, and Meiliya Cahya Yustina, “Ancaman Dan Solusi Serangan Siber Di Indonesia,” *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92, http://ejournal.upi.edu/index.php/TELNECT/.

The BSSN framework additionally offers insights into security measures that electronic system managers can implement. According to the information retrieved from the official website of the National Cyber and Encryption Agency (BSSN) on October 27, 2021,[14] there has been an observed escalation in the frequency of cyberattacks perpetrated by hacker collectives, which are believed to originate from Brazil. The objective pertains to the electronic systems employed by diverse ministries, state entities, military establishments, academic institutions, and other sectors within the nation of Indonesia. The cyber security stakeholders in Indonesia, specifically the electronic system managers of different institutions and organizations, are advised to enhance their knowledge and security measures pertaining to the electronic systems under their management. This can be achieved by employing a range of proactive measures. The following steps were undertaken:

1) In order to mitigate the potential exploitation of vulnerabilities in ports, services, and plugins, it is advisable to deactivate those that are not actively utilized on electronic systems. This precautionary measure aims to prevent unauthorized individuals from taking advantage of these exposed entry points.
2) The implementation of security perimeters, such as a Web Application Firewall (WAF), Intrusion Prevention System (IPS)/Intrusion Detection System, and AntiVirus/Malware, should be undertaken. Additionally, proactive network monitoring should be conducted to identify any potentially malicious activities, such as attempted attacks on managed electronic systems.
3) It is advisable to regularly create backups of your data and electronic systems onto a distinct offline storage system. The task involves recognizing susceptibilities and implementing routine security updates on supervised electronic systems, particularly those pertaining to security perimeters, networks, applications, databases, and operating systems utilized by computers or servers that function as service systems accessible to the general public.
4) It is recommended to frequently update the passwords for administrator and user accounts across all electronic systems, including apps, databases, servers, and other relevant platforms. This should be done using robust passwords and using multifactor authentication measures.
5) It is imperative to do routine security testing on all electronic systems in order to detect vulnerabilities or security deficiencies, and then address and rectify any identified security gaps.

In order to address potential cyberattacks, it is recommended to implement mitigation measures and promptly notify the National Cyber and Encryption Agency (BSSN) through the BSSN Cyber Contact Center. This may be done by sending an email to jasa70@bssn.go.id or by utilizing the telegram platform at https://t.me/helpan70. If one discovers evidence of abnormalities or irregularities.

The KPU also implements proactive measures to predict and mitigate cybercrime. The preventative measures can be implemented through a series of six sequential steps. Firstly, it is important to impart novel insights regarding cybercrime and the realm of the internet, so enhancing the expertise of people. Furthermore, it is imperative to employ a hacker's mindset when devising strategies to safeguard the system. By adopting the perspective of a hacker, one can effectively identify potential vulnerabilities and develop robust countermeasures to mitigate security risks. Furthermore, it is imperative to address and rectify the vulnerabilities present inside the system. Subsequently, it is important to ascertain the laws and regulations that

[14] BSSN, “Indonesia: BSSN Issues Recommendations for Preventing Cyber Attacks,” 29 October, 2021, https://www.dataguidance.com/news/indonesia-bssn-issues-recommendations-preventing-cyber.

safeguard the system against unauthorized individuals, commonly referred to as policy measures. Additionally, the activation of both firewall and antivirus software is recommended to fortify the system's security. It is imperative to consistently spread knowledge and comprehension of these measures as a preventive measure, commencing from the onset of occurrences transpiring on supervised digital platforms.

In the context of Russia, the Bureau of Intelligence and National Security (BIN) plays a crucial role in the prevention, mitigation, and resolution of various threats that pose risks to the nation's security and its broader interests. The Bureau of Intelligence and Investigation (BIN) plays a crucial function as it serves as a primary source of surveillance and information gathering. The Bureau of Information and Navigation (BIN) possesses the duty and jurisdiction to assist the president in crafting development priorities, which encompass the enhancement of human resources and cyber technology.[15] A notable concern within the realm of cybersecurity pertains to the occurrence of cyber assaults targeting a nation's strategic infrastructure. The possible ramifications of cyberattacks pose a significant threat to various facets of contemporary society, with the potential to undermine national stability if not promptly addressed.

Russia's utilization of cyber capabilities extends beyond the domain of technological instruments and information systems. The augmentation of cyber capabilities was executed through the deliberate disruption of Ukraine's electricity infrastructure, resulting in a subsequent deterioration of its cyber domain while concurrently fostering an environment conducive to the acquisition of novel cyber prowess.[16] According to the aggressive realism approach, Russia can be considered a Great Power due to its persistent pursuit of power maximization, with the ultimate objective of establishing hegemony over the Eastern European region.

Factors Influencing the Level of Vulnerability of Election Systems to Cyber Attacks

The field of Information Security has a significant impact on the security of Information System Security. In this context, Information Security dimensions or indicators serve as measures to safeguard information assets from potential attacks. Information security plays a crucial role in ensuring business continuity by mitigating potential threats that may arise. The dimensions or indicators of Information System Security are influential in ensuring the necessity of data security for users of information systems, as it serves to limit the likelihood of data breaches. Furthermore, investigations have been conducted pertaining to cyberattacks against government entities. In order to enhance Information System Security through the prioritization of Information Security, management must undertake a systematic procedure aimed at safeguarding critical and sensitive information. The implementation of information security measures serves the purpose of safeguarding sensitive data from potential attacks that may compromise the overall performance and accomplishments of an organization or individual. The field of Information Security has a significant impact on Information System Security. When customers or consumers have a positive perception of Information Security, it can lead to enhanced quality in

[15] *Fathika* Anjani Firman, "Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia" (UNIKOM University, 2018), https://repository.unikom.ac.id/59424/.

[16] M Yusuf Samad and Pratama Dahlian Persadha, "Memahami Perang Siber Rusia Dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats," *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi* 24, no. 2 (2022): 135–46, http://dx.doi.org/10.17933/iptekkom.24.2.2022.135-146.

the implementation of Information System Security within an organization. Additionally, establishing organizational guidelines can be an effective strategy for managing information security effectively.

The influence of networks on Information System Security is a significant consideration, particularly in relation to internet-based dimensions or indicators of Information Security. This is due to the inherent characteristics of internet computer networks, which are both public and global, and hence pose inherent risks to security. When transmitting data from one computer to another over the internet, the data traverse multiple intermediary computers, so exposing it to potential interception or manipulation by other internet users. The dimensions or indicators of Information System Security encompass the capacity to consistently access data, as well as the preservation of confidentiality and integrity of the information stored. These aspects are crucial in all organizations as they serve to mitigate potential errors in usage, as well as prevent any harm or loss of business data. Such incidents can significantly impede the primary operational activities of a company.[17]

In order to ensure the security of an information system, it is imperative for management to prioritize the protection of network equipment, the organization itself, the network and its contents, as well as the proficiency in utilizing the network to effectively fulfill the organization's data communication function. The influence of networks on Information System Security is significant. When customers or consumers have a positive perception of Information Security, it can enhance the level of security guarantees. This, in turn, plays a crucial role in establishing trust by alleviating consumer apprehensions regarding the misuse of personal data and the vulnerability of data transactions. When the level of security assurance reaches a satisfactory standard and aligns with consumer expectations, individuals may be inclined to divulge their personal information and make purchases with a sense of confidence in the security measures in place. The subject of discussion pertains to the field of Information Systems Security.

CONCLUSION

The prevalence of cyberattacks targeting electoral processes in many nations is a substantial and pressing challenge. In the context of elections, safeguarding against cyberattacks necessitates a collaborative effort by governmental entities, electoral institutions, and cybersecurity professionals. Efforts aimed at enhancing the security of election systems, providing training to users on the identification of cyberattacks, and fostering public awareness regarding these dangers are crucial measures for upholding the integrity and trustworthiness of the democratic process. The novelty of cyberattacks lies not only in the media employed, but also in the absence of legal frameworks and processes capable of effectively classifying the illegality of various techniques. It is imperative for the government to establish a comprehensive and stringent framework of penalties to address instances of defamation, disinformation, and related transgressions perpetrated by political campaign teams or candidates themselves. In addition, it is imperative to allocate resources towards enhancing cybersecurity measures, encompassing the fortification of current software and networks, with the aim of mitigating the potential risks associated with unauthorized access to the federal voting system. Active participation from institutions such as the Department of Homeland Security, the Infrastructure Security

[17] Aryuni Yuliantiningsih, "Analisis Doktrin Perang Yang Adil (Just War) Dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008," *Kosmik Hukum* 21, no. 3 (2021): 175, https://doi.org/10.30595/kosmikhukum.v21i3.10613.

Agency, and state governments is necessary in this regard. In conclusion, it is imperative for civil society to enhance its vigilance. This is due to the fact that voters now have direct access to information, thereby underscoring the need of education. This objective can be accomplished by several measures, including verifying the accuracy of information, enhancing one's proficiency in digital literacy, and avoiding the confinement of one's perspectives within social media echo chambers. These echo chambers tend to propagate unverified claims and foster polarization by disseminating misleading narratives about competing viewpoints.

REFERENCES

Anjani Firman, Fathika. "Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia." UNIKOM University, 2018. https://repository.unikom.ac.id/59424/.

Blayne Haggart, Jan Aart Scholte, Natasha Tusikov. *Power and Authority in Internet Governance: Return of the State?* New York: Taylor & Francis, 2021.

BSSN. "Indonesia: BSSN Issues Recommendations for Preventing Cyber Attacks." 29 October, 2021. https://www.dataguidance.com/news/indonesia-bssn-issues-recommendations-preventing-cyber.

Clough, Jonathan. "A WORLD OF DIFFERENCE: THE BUDAPEST CONVENTION ON CYBERCRIME AND THE CHALLENGES OF HARMONISATION." *Monash University Law Review* 40, no. 3 (2014): 698. http://classic.austlii.edu.au/au/journals/MonashULawRw/2014/28.pdf.

Jose, Hino Samuel. "Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 Di Forum Multilateral." *Populika* 9, no. 2 (2021): 70–85. https://doi.org/10.37631/populika.v9i2.390.

Kaskus. "Serangan DoS Pada Situs Kaskus Oleh Komunitas YogyaFree," 2016. https://www.kaskus.co.id/thread/56c2c8d69a09515e5e8b4567/serangan-dos-pada-situs-kaskus-oleh-komunitas-yogyafree.

Nurul, Shinta, Shynta Anggrainy, and Siska Aprelyani. "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)." *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)* Vol. 3, no. No. 5 (2022): 564–73.

Parulian, Sahat, Devi Anassalifa Pratiwi, and Meiliya Cahya Yustina. "Ancaman Dan Solusi Serangan Siber Di Indonesia." *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)* 1, no. 2 (2021): 85–92. http://ejournal.upi.edu/index.php/TELNECT/.

Pratama, M Syadli, Fetri Miftach, and Yusuf Ali. "The Cyber Security Strategy of General Elections Commission in Facing the General Election 2019." *Jurnal Prodi Perang Asimetris* 4, no. 3 (2018): 77–94.

Samad, M Yusuf, and Pratama Dahlian Persadha. "Memahami Perang Siber Rusia Dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats." *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi* 24, no. 2 (2022): 135–46. http://dx.doi.org/10.17933/iptekkom.24.2.2022.135-146.

Sandrawati, Nyoman Amie. "Antisipasi Cybercrime Dan Kesenjangan Digital Dalam Penerapan TIK Di KPU." *Electoral Governance Jurnal Tata Kelola Pemilu Indonesia* 3, no. 2 (2022): 232–57.

Snyder, H. "Literature Review as a Research Methodology: An Overview and Guidelines." *Journal of Business Research*, 2019, 333–39. https://doi.org/https://doi.org/10.1016/j.jbusres.2019.07.039.

Soekanto, Soerjono. *Faktor-Faktor Yang Mempengaruhi Penegakan Hukum*. Jakarta: PT Rajawali Pers, 2015.

Statistics, National Center for Education. "Protecting Your System: Information Security," 2023. https://nces.ed.gov/pubs98/safetech/chapter6.asp.

Suharto, Miko Aditiya, and Maria Novita Apriyani. "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional." *Risalah Hukum* 17 (2021): 98–107. https://doi.org/10.30872/risalah.v17i2.705.

Union, International Telecommunication. “Global Cybersecurity Index (GCI) 2017.” Geneva, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Yuliantiningsih, Aryuni. “Analisis Doktrin Perang Yang Adil (Just War) Dalam Kasus Serangan Siber Rusia Terhadap Georgia Tahun 2008.” *Kosmik Hukum* 21, no. 3 (2021): 175. https://doi.org/10.30595/kosmikhukum.v21i3.10613.