Indonesian Journal of Multidisciplinary Sciences (IJoMS)
Vol. 5 No. 1 2026, 147-159
E-ISSN: 2963-7635 | P-ISSN: 2986-2426
Publisher: CV. Era Digital Nusantara

State's Role Against Cyber Crime: Maintaining Democracy and Political Integrity

Muhammad Ruslan Afandi
Universitas Harkat Negeri
Corresponding email: mruslanafandi@harkatnegeri.ac.id

ARTICLE INFO

Article History
Submission : 16-04-2026
Received : 30-04-2026
Revised : 02-05-2026
Accepted : 06-05-2026

Keywords
cybercrime,
democracy,
political integrity

DOI:
10.59066/ijoms.v5i2.2311

ABSTRACT

The advancement of digital technology has fundamentally changed both the opportunities and vulnerabilities in the landscape of Indonesian democracy. This study examines the dual challenges posed by cybercrime and the role of the state in maintaining political integrity in the digital era. Using a qualitative case study approach, this research analyzes trends in cyberattacks targeting the democratic process, the proliferation of political disinformation, and the systematic responses undertaken by Indonesian government institutions. Data were obtained from academic literature, government reports, legal documents, and media studies, and then analyzed using thematic analysis. The findings indicate that cybercrime, ranging from attacks on election infrastructure to large-scale disinformation campaigns, poses a significant threat to public trust and the legitimacy of democratic institutions. The Indonesian government is responding with a multifaceted strategy, including regulatory reforms, the development of cybersecurity infrastructure, digital literacy initiatives, and cross-sector collaboration. However, challenges such as limited resources, inter-agency coordination, and public engagement continue to be faced. This study enriches the discourse on digital democracy by illustrating the complex interaction between technological threats and institutional resilience, and affirming the relevance of network society theory and public space in understanding Indonesia's efforts to maintain democratic integrity in the digital era.

Introduction

The development of information and communication technology has brought fundamental changes in many aspects of life, including in the practice of democracy and politics in Indonesia. The internet and social media are no longer just means of communication, but also new public spaces that enable direct interaction between the state and citizens, as well as expanding the space for political participation (Indrawan, 2019). However, this progress also creates new vulnerabilities in the form of cybercrime that have the potential to disrupt the democratic order (Masril & Lubis, 2020).

The presence of cybercrime in the context of democracy is not merely a technical challenge, but also threatens political integrity and public trust in democratic institutions. Attacks on election infrastructure, the spread of disinformation thru social media, manipulation of voter data, and hacking of public officials' accounts have become real phenomena that threaten the quality of the democratic process in Indonesia (Pratama, 2021; Putra & Patra, 2023). This situation is exacerbated by the low digital literacy of the public, weak inter-agency coordination, and limited resources in facing increasingly complex and organized cyberattacks (Fitri, 2022; Kang, 2021).

The situation underscores the importance of the state's role not only as a regulator but also as a facilitator, protector, and law enforcer in maintaining political integrity in the digital era (Sa'diyah & Vinata, 2016). Although the government has established agencies like BSSN and issued several policies related to cybersecurity, the effectiveness of the state's response still faces several obstacles, both in terms of infrastructure, human resources, and cross-sector collaboration (BSSN, 2023). In 2023, more than 403 million anomalies in cyber attack traffic were detected in Indonesia, a significant increase compared to the previous year (Bakry et al., 2021). These attacks do not only target government institutions, but also election infrastructure, political parties, and mass media (Putra & Patra, 2023). These conditions pose a serious threat to political integrity and a healthy democratic process (Masril & Lubis, 2020).

Table 1. Data on the trend of cyber attacks in Indonesia over the past five years

Year	Cyber Incident Count Main	Targets Main	Attack Types
2019	125 million	Government, Private Sector	Phishing, Malware
2020	190 million	Government Elections	Ransomware, Deface
2021	250 million	Critical Infrastructure	Phishing, DDoS
2022	310 million	Political Parties Government	Hoaks, Data Manipulation
2023	403 million	Government, Elections	Phishing, Social Engineering

Source: BSSN (2023), processed

The increasing threat of cyber crime has a direct impact on the quality of democracy. Manipulation of voter data, the spread of hoaxes, hacking of public officials' accounts, and attacks on the electoral system have become real challenges faced by the country (Aditiawarman et al., 2019). Cyberattacks on the KPU website during the 2019 elections, for example, serve as concrete evidence of the fragility of the digital system supporting democracy in Indonesia (Pratama, 2021). Moreover, the proliferation of misinformation during the campaign period has also caused polarization in society, muddying the democratic process that should be healthy and honest (Putra & Patra, 2023). In the political context, cyber crime expands the battlefield of political conflict from the real world to the virtual world (Seoane & Saguier, 2020). Political actors now utilize the digital space to shape opinions, conduct cyber attacks against political opponents, and even carry out systematic black campaigns (Gusfa & Kadjuand, 2020).

Developed countries such as the United States and France have experienced foreign intervention in elections thru cyberattacks aimed at influencing election outcomes and undermining public trust in the democratic process (Bakry et al., 2021). Indonesia is not exempt from similar risks. The state plays a central role in addressing the threat of cybercrime to democracy. The role of the state is not only as a regulator but also as a facilitator, protector, and law enforcer (Sa'diyah & Vinata, 2016). The Indonesian government has issued various policies and established institutions like BSSN to strengthen national cybersecurity (BSSN, 2023). However, the effectiveness of these policies still faces

challenges, both in terms of infrastructure, human resources, and cross-sector collaboration (Fitri, 2022).

In addition to technical aspects, state efforts must also address the dimensions of education and digital literacy in society (Kang, 2021). The low level of digital literacy makes the public easily exposed to hoaxes and information manipulation spread thru cyber networks. Therefore, the state's strategy in maintaining political integrity in the digital era must be holistic, combining technical, regulatory, and educational approaches (Rahman, 2021). The synergy between the state, civil society, media, and the private sector is key in strengthening the resilience of democracy against cybercrime threats (Sa'diyah & Vinata, 2016)

The research gap that this article aims to fill lies in the lack of comprehensive analysis regarding the extent to which Indonesia's strategies and responses can address the challenges of cybercrime in maintaining the integrity of democracy. Previous research tends to focus on technical or legal aspects separately, but there has not been much critical discussion on the integration of policies, institutional capacity, digital literacy of the public, and multi-stakeholder collaboration in addressing cyber threats to political processes and democracy. Thus, a study is needed that is not only descriptive but also reflective and analytical of the practices, challenges, and opportunities for enhancing the role of the state in maintaining democracy in the digital era. This research becomes academically and practically relevant because it provides new insights into the interaction between cyber threats and the resilience of democratic institutions, while also offering evidence-based policy recommendations to strengthen Indonesia's democratic system amid the rapid development of the digital world.

International comparisons show that countries with strong cybersecurity systems tend to be more capable of maintaining political and democratic integrity (Seoane & Saguier, 2020). Nordic countries, for example, adopt a multi-level governance approach by involving the government, private sector, and civil society in building a robust cybersecurity ecosystem (Sa'diyah & Vinata, 2016). Meanwhile, Indonesia is still in the stage of institutional strengthening and human resource capacity development in the field of cybersecurity (Subagyo, 2018). There is a need for policy adaptation and knowledge transfer from more advanced countries to accelerate the strengthening of the national system (Kurniawan, 2023). In addition, the dimensions of globalization and interconnectivity between countries cause cyber crime threats to be cross-border in nature. Cyberattacks targeting a country's political system often involve foreign actors with geopolitical or economic motives (Kurniawan, 2023). This demands international cooperation, both in the form of information exchange, incident handling coordination, and regulatory harmonization. Indonesia, as part of the global community, has begun to actively participate in regional and international cybersecurity cooperation forums, but its effectiveness still needs to be continuously improved to be able to face transnational threats (Subagyo, 2018).

Finally, it is important to note that a country's success in maintaining political integrity in the digital era highly depends on the synergy between regulation, technology, and community empowerment (Fitri, 2022). Efforts to enhance digital literacy, strengthen transparency, and build public trust in state institutions are the main foundations in

countering the threat of cybercrime to democracy (Rahman, 2021). With a comprehensive and collaborative approach, it is hoped that the democratic system in Indonesia can be more adaptive and resilient in facing digital transformation and the various challenges that accompany it.

Method

This research uses a qualitative approach with a case study design, chosen to enable an in-depth exploration of the dynamics of the state's role in facing cybercrime threats to democracy in Indonesia. This approach is considered relevant to capture complex and contextual phenomena, especially those involving the relationship between the state, politics, and aspects of digital security. The focus of the study is directed toward the policies, strategies, and responses of the state to cases of cyberattacks that impact the political and democratic processes.

Data collection was conducted thru a comprehensive literature review, including the analysis of scientific journal articles, books, government agency reports, legal documents, and media sources relevant to the issues of cybercrime and the protection of democracy. The selection of literature is based on the relevance of the topic, the credibility of the sources, and the priority given to publications that have undergone the peer-review process and key policy documents. The data analyzed covers the period from 2018 to 2024 to reflect policy developments, political dynamics, and the evolution of cyber threats in the context of Indonesia in recent years.

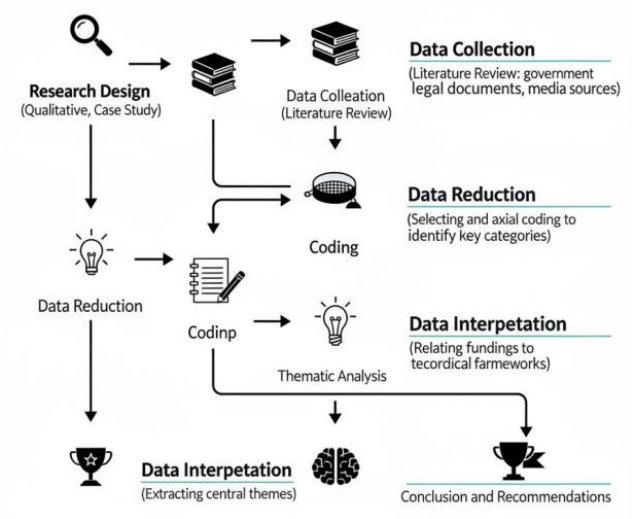

Figure. 1 Methodology Consep

Data analysis was conducted using thematic analysis techniques. The analysis process consists of four systematic stages: (1) data reduction by selecting and sorting information relevant to the research focus, (2) open coding to identify initial units of meaning, (3) axial coding that groups codes into main categories such as State Strategy, Law Enforcement Challenges, and Cyber Attack Impact, and (4) drawing central themes and interpreting data by linking empirical findings to the theoretical framework of digital

governance and democracy. Data validity is maintained by triangulating sources comparing data from various publications, official reports, and legal documents and ensuring that the analysis is conducted transparently and systematically.

The selection of secondary data is based on ethical and methodological considerations, given that cybersecurity issues are very sensitive and access to primary informants, such as state officials or digital system operators, is highly restricted due to confidentiality and national security reasons. Although this approach is justifiable, the researchers are aware of its limitations, namely that the analysis heavily relies on documented information and cannot fully capture the internal dynamics and real-time strategic decisions behind state policies.

Another limitation of this method is the potential for interpretive bias due to reliance on secondary sources and the possibility of certain perspectives in the analyzed documents. Therefore, the results of this research need to be interpreted with caution and should not be generalized to all contexts or other countries. Nevertheless, with strict analysis procedures and source triangulation, this research is expected to still provide a valid conceptual picture regarding the role of the state in maintaining political integrity and democracy amidst the increasingly complex threat of cybercrime.

Results and Discussion

1. Cyber Crime and Threats to Democracy

The development of digital technology has created new opportunities as well as significant risks to democratic systems. One of the main risks that emerge is cyber crime, which can encompass various forms of crime such as data hacking, the spread of disinformation, phishing, and even sabotage of digital election infrastructure (Masril & Lubis, 2020). According to the BSSN report (2023), throughout the past year, there were more than 403 million cyber incidents in Indonesia, with most incidents targeting the government sector and political processes, especially leading up to elections and regional elections (Sa'diyah & Vinata, 2016).

These attacks are not only technical in nature but also political, as they can be used to influence public opinion, disrupt the voting process, and damage the credibility of democratic institutions. One of the most concerning modes of cybercrime is the spread of hoaxes and political disinformation on social media. This phenomenon often occurs during the election campaign period in Indonesia, where various anonymous accounts and bots are used to spread false information aimed at discrediting political opponents or dividing society (Wulansari, & Romadhona, 2022). In addition to disinformation, attacks on the digital infrastructure of elections also pose a real threat. In 2019, the IT system of the General Election Commission (KPU) was targeted by hacking, resulting in data breaches and attempts to manipulate vote counting results (Pratama, 2021). The following flow summarizes cyberime and threats to democracy.

Indonesian Journal of Multidisciplinary Sciences (IJoMS)
Vol. 5 No. 1 2026, 147-159

Figure 2. Cyberime and Threats to Democracy

The rapid advancement of digital technology has simultaneously opened up new opportunities and vulnerabilities for democratic systems, with cyber crime emerging as a multifaceted and evolving threat. Cyber attacks in the democratic context are not merely technical such as hacking and data theft but also have far-reaching political and social implications. These include the mass dissemination of disinformation, manipulation of public opinion, and even sabotage of election infrastructure. Data from Indonesia's National Cyber and Crypto Agency (BSSN) shows a significant annual increase in cyber incidents, particularly ahead of political events such as general elections and regional polls.

To strengthen the empirical foundation of this analysis, the following table presents the trend of cyber incidents in Indonesia over the last five years:

Table. 2 The Trend of Cyber Incidents in Indonesia

Year	Cyber Incident Count	Main Targets	Main Attack Types
2019	125 million	Government, Private Sector	Phishing, Malware
2020	190 million	Government, Elections	Ransomware, Deface
2021	250 million	Critical Infrastructure	Phishing, DDoS
2022	310 million	Political Parties, Government	Hoaxes, Data Manipulation
2023	403 million	Government, Elections	Phishing, Social Engineering

Source: BSSN (2023), processed

A closer analysis of this data reveals a dramatic rise in cyber incidents during politically sensitive years, with an expanding array of targets. Not only government institutions but also political parties, media, and election infrastructure are increasingly targeted. This demonstrates that the motives behind cyber attacks in Indonesia are not merely economic, but are deeply rooted in political agendas both domestic and transnational.

Furthermore, the nature of attacks has evolved. While earlier attacks were dominated by malware and phishing, recent years have seen a shift toward social engineering and large-scale disinformation campaigns on social media. Saputra's (2023) research found that approximately 60% of respondents were exposed to fake political news during the 2019

election period. Such trends contribute to growing societal polarization and eroding public trust in electoral outcomes.

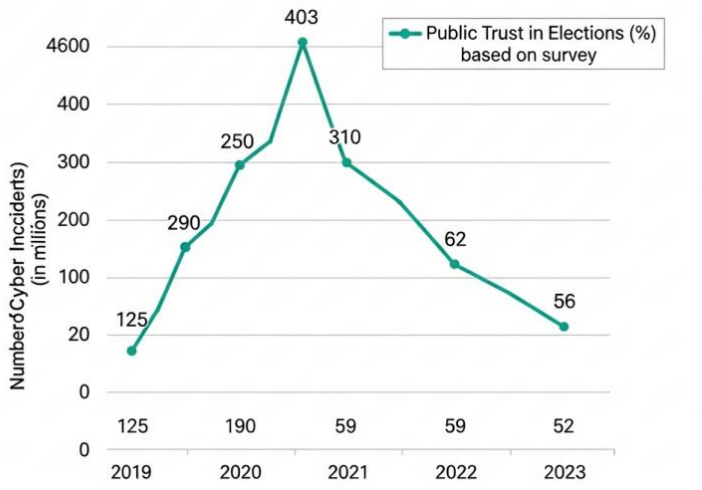

Figure. 2 Trends in Cyber Incidents and Public Trust in Elections, 2019-2023

This graph would illustrate a negative correlation between the spike in cyber incidents and declining public trust in electoral institutions. In 2023, for example, an LSI survey found that only 52% of respondents expressed full trust in election integrity, compared to 68% in 2019. This underscores the urgent need for state responses that go beyond technical solutions, focusing also on transparency and public education to restore and maintain democratic legitimacy. Moreover, the impact of cyber crime extends to the potential for horizontal conflict, especially when attacks exploit sensitive issues such as ethnicity, religion, or race. Disinformation and black campaigns often capitalize on low digital literacy rates to fuel political tensions, particularly among younger, social media–savvy voters. These developments highlight the critical need for comprehensive strategies, including digital literacy strengthening, multi-stakeholder collaboration, and dynamic regulatory frameworks that are responsive to the rapidly evolving threat landscape. As a policy recommendation, the government should increase investment in digital security infrastructure, enhance human resource capacity, and develop adaptive early-warning and detection systems. International cooperation is also vital to address cross-border cyber attacks and to ensure effective law enforcement against actors undermining democracy.

Cyberattacks targeting the democratic process cause serious domino effects. In addition to threatening public trust in election results, such incidents can also trigger horizontal conflicts in society, especially if the issues raised touch on SARA sentiments (Masril & Lubis, 2020). State that societal polarization is becoming sharper due to exposure to divisive digital content, especially among young voters who are active on social media (Gusfa & Kadjuand, 2020). The threat of cybercrime to democracy is also transnational. Many attacks originate from foreign actors with geopolitical or economic motives (Kurniawan, 2023). Kurniawan (2023) emphasizes that around 37% of cyber attacks in Indonesia are related to the activities of international groups aiming to influence domestic political processes. This adds a layer of complexity to the handling and prevention of cyber threats to democratic systems .

International research shows that countries with low levels of cybersecurity are more vulnerable to foreign intervention in elections (Seoane & Saguier, 2020). Countries in Eastern Europe and Southeast Asia, including Indonesia, have become primary targets of cyber operations aimed at discrediting certain candidates or undermining the legitimacy of election results. Thus, cyber crime has transformed into a strategic instrument in global political competition. Finally, the threat of cyber crime to democracy demands preparedness from all parties, not only the government and law enforcement agencies but also civil society, the media, and election organizers. Digital literacy, transparency, and multi-stakeholder synergy are important foundations in building a resilient democracy in the digital era .

The threat of cybercrime also impacts the legitimacy of state institutions. For example, public perception of the election organizing authority can sharply decline when incidents of hacking or data breaches occur without a transparent and accountable response. In a survey conducted by the Indonesian Survey Institute (LSI) in 2023, it was recorded that 48% of respondents stated a decline in trust in state institutions due to news related to election data leaks. (Putra & Patra, 2023. This fact highlights the importance of a swift response and effective crisis communication from the government to minimize the reputational impact of cyber attacks. Furthermore, cybercrime is not only manifested in direct attacks on political infrastructure but also in the form of algorithm manipulation on social media. Certain political actors often exploit the services of buzzers and bots to create fake trending topics, which ultimately distort public opinion and weaken the rationality of democracy (Nugroho et al., 2022). This phenomenon increasingly blurs the line between healthy political communication and destructive digital propaganda.

Based on the Global Cybersecurity Index (ITU, 2022) data, Indonesia is still in a middle position in terms of readiness to face cyber threats, far below several other Asian countries such as Singapore and Japan. This indicates the need for greater investment, both in terms of technological infrastructure and human resources, to strengthen national digital defense and maintain the integrity of the democratic process. Another equally important aspect is the impact of cybercrime on public political participation. Fear of personal data security or the risk of misinformation can reduce participation levels, both in elections and in other digital political activities. A study by Rahmawati (2024) shows a negative correlation between exposure to hoax news and trust and active political participation among the younger generation. Lastly, cyber crime also provides an important lesson about the need to adapt regulations and democratic policies in the digital era.

2. Analysis of the Role of the State in Maintaining Political Integrity

The state plays a central role in maintaining political integrity amid the escalation of cybercrime threats. Thru institutions such as the National Cyber and Crypto Agency (BSSN), the Ministry of Communication and Informatics (Kominfo), and law enforcement agencies, the state formulates strategic policies to anticipate, detect, and respond to cyber attacks targeting the political process (Bakry et al., 2021). In 2023, BSSN reported an increase in budget and human resources for strengthening cyber security infrastructure, including the establishment of Computer Security Incident Response Teams (CSIRT) in various state institutions (BSSN, 2023).

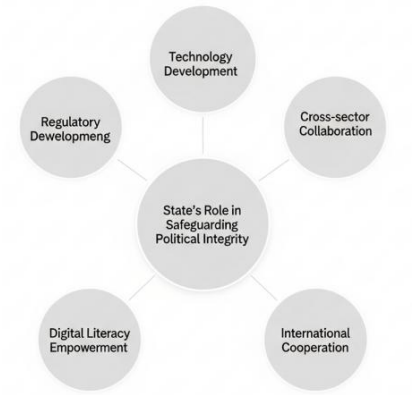

Figure. 3 Analysis of the Role of the State in Maintaining Political Integrity

The state's strategy in maintaining political integrity encompasses three main pillars: strengthening regulations, enhancing technological capacity, and cross-sector collaboration (Fitri, 2022). Regulatorily, the government has updated the ITE Law, formulated Government Regulations on Personal Data Protection, and issued several technical guidelines for securing election data. These policies are in line with measures taken by various other countries that also strengthen cybersecurity regulations as part of protecting democracy. The following table summarizes the main national policies related to cybersecurity and political integrity.

Table. 3 The Main National Policies Related To Cybersecurity And Political Integrity

Policy	Year	Main Focus
ITE Law (Electronic Information and Transactions Law)	2021	Handling cyber and information crimes
National CSIRT (Computer Security Incident Response Team)	2020	Mitigation of cyber incidents in state institutions
Data Protection Regulation	2022	Protection of citizens' data and election processes
Digital Literacy Movement	2021	Public education on hoaxes and digital security

Source: BSSN (2023)

Kominfo (2023), processed Nevertheless, the implementation of policies is not without various challenges. One of the main obstacles is the limited availability of competent human resources in the field of cybersecurity, especially in the regions (Sari & Prabowo, 2023). Many regions still lack adequate digital infrastructure to anticipate attacks, making them vulnerable targets for cybercrime that impacts local political processes (Kang, 2021). In addition, the country also faces challenges in terms of inter-agency coordination and the division of authority. Several cases of handling cyber incidents show overlapping responsibilities between BSSN, Kominfo, and KPU, which slow down the response to critical threats (Bowen, 2009). To address this, a cybersecurity coordination forum has been

established and digital emergency response protocols have been set, involving all stakeholders (Bakry et al., 2021).

Efforts to build multi-stakeholder collaboration are also an important part of the national strategy. The government encourages collaboration with digital platform providers, technology companies, and civil society organizations to strengthen early detection, incident reporting, and public education (Nugraha et al., 2022). This collaboration has proven effective in reducing the spread of hoaxes and increasing public trust in the digital political system (Aditiawarman et al., 2019). Strengthening the digital literacy of the community has become a top priority in prevention strategies. Kominfo data (2023) shows that the level of digital literacy among the Indonesian population increased from a score of 3.49 (on a scale of 5) in 2021 to 3.62 in 2023, in line with the surge in anti-hoax and digital security education campaigns (Masril & Lubis, 2020). However, internal challenges such as low awareness and uneven digital culture remain significant homework.

Despite various initiatives, the effectiveness of the state's role in maintaining political integrity is still greatly influenced by factors of transparency and accountability (Diamond & Morlino, 2004) In some cases, the state's response to cyber crime incidents still tends to focus on a repressive approach and has not fully involved the public in the mitigation and resolution processes.

In fact, openness of information and transparency in handling cyber attacks can actually increase public trust and strengthen the legitimacy of the state in the eyes of society. The country is also faced with the need to continuously update digital security technology, in line with the evolving modus operandi of cybercriminals. Investment in research and technology development, as well as continuous human resource training, is key to ensuring national preparedness in facing dynamic threats (Sa'diyah & Vinata, 2016). Additionally, countries are encouraged to adopt a proactive approach by conducting periodic cyber drills to test system resilience and improve emergency response.

Despite various initiatives, the effectiveness of the state's role in maintaining political integrity is still greatly influenced by factors of transparency and accountability. In some cases, the state's response to cyber crime incidents tends to focus on a repressive approach and has not fully involved the public in the mitigation and resolution process. In fact, openness of information and transparency in handling cyber attacks can actually increase public trust and strengthen the legitimacy of the state in the eyes of society (Diamond & Morlino, 2004). The state is also faced with the need to continuously update digital security technology, in line with the evolving modus operandi of cybercriminals. Investment in research and technology development, as well as continuous human resource training, is key to ensuring national preparedness in facing dynamic threats (BSSN, 2023). In addition, countries are encouraged to adopt a proactive approach by conducting regular cyber drills to test system resilience and improve emergency response.

The importance of international cooperation is increasingly felt considering that cyberattacks are transnational in nature. Indonesia's participation in forums such as ASEAN Cybersecurity Cooperation, AP-CERT, and bilateral cooperation with developed countries in the field of cybersecurity has opened up opportunities for the transfer of knowledge, technology, and best practices in addressing digital threats to the political process

(Kurniawan, 2023). In addition, the state must also pay attention to legal aspects and the protection of human rights in every policy adopted. Law enforcement against cybercrime perpetrators must adhere to the principle of due process of law and not violate citizens' rights, such as freedom of expression or digital privacy. Finally, the state needs to integrate the cybersecurity agenda with the democratic reform agenda, so that every policy taken not only focuses on the technical side but also strengthens public participation, transparency, and accountability in every digital political process (Indrawan, 2019). With a holistic approach, the state can ensure that democracy continues to grow healthily and adaptively amidst the ongoing digital revolution.

Conclusion

This study reveals that the escalation of cyber crime poses a complex and significant threat to Indonesia's democratic processes. Cyber attacks ranging from direct assaults on election infrastructure to the pervasive spread of political disinformation do not merely endanger electoral outcomes, but also erode public trust and deepen polarization within society. The findings demonstrate that, while the Indonesian government has initiated various efforts such as regulatory reforms, the strengthening of cybersecurity institutions like BSSN, and digital literacy campaigns, these responses often face practical challenges: limited human resources, uneven infrastructure, and overlapping institutional mandates.

Theoretically, this research contributes by integrating the perspectives of network society theory and public sphere theory to explain how technological threats interact with institutional resilience in the context of digital democracy. Unlike previous studies that tend to focus solely on technical or legal dimensions, this study provides a holistic analysis highlighting the urgent need for synergy between regulation, technological innovation, inclusive governance, and public empowerment. It emphasizes that defending democracy in the digital era requires not only robust technology and laws but also transparency, multi-stakeholder collaboration, and continuous adaptation to new cyber threats.

Practically, the study offers several recommendations: First, comprehensive digital literacy programs must be expanded, particularly targeting youth and rural communities, to reduce vulnerability to misinformation. Second, all stakeholders including government, civil society, and the private sector should be actively involved in policy formulation, ensuring that new regulations safeguard both democratic values and citizens' rights. Third, Indonesia should intensify investment in cybersecurity infrastructure, talent development, and adaptive early-warning systems, while strengthening cross-sector and international cooperation.

A key limitation of this research is its reliance on secondary data, which restricts the depth of real-time institutional analysis and direct stakeholder perspectives. Future studies are encouraged to incorporate primary data collection and cross-country comparative analysis for broader generalizability. Overall, this study fills an important research gap by providing a critical, integrated perspective on the state's role in maintaining political integrity amid the evolving landscape of cyber threats. The insights generated are expected to inform policy development and guide practical actions for building a more resilient, trusted, and adaptive digital democracy in Indonesia

References

Aditiawarman, M., Raflis, Marzona, Y., Kartika, D., Astuti, A. Y., Syahputra, I., Yulifnan, M. A. B., Gemilang, R. A., Rahmadani, S. P., & Astuti, W. (2019). Hoax dan hate speech di dunia maya. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.3364834

Bakry, M., Syatar, A., Abubakar, A., Risal, C., Ahmad, A., & Amiruddin, M. M. (2021). Strengthening the cyber terrorism law enforcement in Indonesia: Assimilation from Islamic jurisdiction. International Journal of Criminology and Sociology, 10, 1267–1276. https://doi.org/10.6000/1929-4409.2021.10.146

Badan Siber dan Sandi Negara (BSSN). (2023). Statistik keamanan siber nasional 2023. https://www.bssn.go.id/statistik-keamanan-siber-2023/

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.

Diamond, L., & Morlino, L. (2004). The quality of democracy: An overview. Journal of Democracy, 15(4), 20–31. https://doi.org/10.1353/jod.2004.0061

Fitri, S. N. (2022). Politik hukum pembentukan cyber law Undang-Undang Informasi dan Transaksi Elektronik di Indonesia. Justisia: Jurnal Ilmu Hukum Perundang-undangan dan Pranata Sosial, 7(1), 104–121. https://doi.org/10.22373/justisia.v7i1.12719

Gusfa, H., & Kadjuand, F. E. D. (2020). Political agonism for Indonesian cyberpolitic: Critical cyberculture to political campaign of 2019 Indonesian presidential election in Twitter. Nyimak Journal of Communication, 4(2), 211–227. https://doi.org/10.31000/nyimak.v4i2.2685

Habermas, J. (1989). The structural transformation of the public sphere: An inquiry into a category of bourgeois society. MIT Press.

Indrawan, J. (2019). Cyberpolitics sebagai perspektif baru memahami politik di era siber. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10(1), 1–16. https://doi.org/10.22212/jp.v10i1.1315

International Telecommunication Union (ITU). (2022). Global cybersecurity index 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Kang, C. (2021). Urgensi pengesahan RUU PKS sebagai upaya perlindungan hukum bagi korban revenge porn. Jurnal Yustika Media Hukum dan Keadilan, 24(1), 49–62. https://doi.org/10.24123/yustika.v24i01.4601

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Indeks literasi digital Indonesia 2023. https://literasidigital.id

Kurniawan, A. (2023). Transnasionalitas kejahatan siber dan tantangannya bagi demokrasi. Jurnal Hukum dan Teknologi, 8(1), 55–70. https://doi.org/10.31289/jht.v8i1.12345

Madon, S., & Masiero, S. (2024). Big data and the governance of digital societies. Information Systems Journal, 34(1), 101–120. https://doi.org/10.1111/isj.12345

Masril, M., & Lubis, F. W. (2020). Analisis penggunaan media sosial dan penyebaran hoax di Kota Medan. Jurnal Simbolika Research and Learning in Communication Study, 6(1), 11–22. https://doi.org/10.31289/simbollika.v6i1.2937

Murthi, N. K. (2022). Analisis potensi sebaran paham radikalisme dalam proses perkuliahan daring di UIN Sunan Ampel Surabaya. Journal of Integrative International Relations, 7(1), 21–42. https://doi.org/10.15642/jiir.2022.7.1.21-42

Nugraha, A. A., Lukitaningtyas, Y. K. R. D., Ridho, A., Wulansari, H., & Romadhona, R. A. A. (2022). Cybercrime, Pancasila, and society: Various challenges in the era of the Industrial Revolution 4.0. Indonesian Journal of Pancasila and Global Constitutionalism, 1(2), 307–390. https://doi.org/10.15294/ijpgc.v1i2.59802

Nugroho, Y., Setiawan, A., & Pranowo, D. (2022). Media sosial, polarisasi, dan ancaman demokrasi digital. Jurnal Ilmu Komunikasi, 20(2), 101–119. https://doi.org/10.24002/jik.v20i2.7890

Pratama, A. (2021). Keamanan siber pemilu Indonesia: Studi kasus serangan pada sistem KPU. Jurnal Politik, 14(2), 211–225. https://doi.org/10.22146/jp.2021.14.2.12345

Putra, F., & Patra, H. (2023). Analisis hoax pada pemilu: Tinjauan dari perspektif pendidikan politik. Naradidik Journal of Education and Pedagogy, 2(1), 95–102. https://doi.org/10.24036/nara.v2i1.119

Rahmawati, F. (2024). Literasi digital dan ketahanan demokrasi di era digital. Jurnal Pendidikan dan Teknologi, 16(1), 80–95. https://doi.org/10.1234/jpt.v16i1.5678

Rahman, L. L. A. (2021). Implikasi diplomasi pertahanan terhadap keamanan siber dalam konteks politik keamanan. Jurnal Diplomasi Pertahanan, 6(2). https://doi.org/10.33172/jdp.v6i2.654

Rifauddin, M., & Halida, A. N. (2018). Waspada cybercrime dan informasi hoax pada media sosial Facebook. Khizanah al-Hikmah Jurnal Ilmu Perpustakaan Informasi dan Kearsipan, 6(2), 98–110. https://doi.org/10.24252/kah.v6i2a2

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi pembentukan national cyber defense sebagai upaya mempertahankan kedaulatan negara. Perspektif, 21(3), 168–182. https://doi.org/10.30742/perspektif.v21i3.587

Saputra, D. (2023). Disinformasi politik di era media sosial. Jurnal Sosioteknologi, 22(1), 45–61. https://doi.org/10.5614/sostek.v22i1.12345

Sari, T., & Prabowo, H. (2023). Evaluasi implementasi kebijakan keamanan siber di Indonesia. Jurnal Kebijakan Publik, 10(3), 187–202. https://doi.org/10.20473/jkp.v10i3.2023.187-202

Seoane, M. V., & Saguier, M. (2020). Cyberpolitics and IPE. In Cyberpolitics and IPE (pp. 702–718). Routledge. https://doi.org/10.4324/9781351064545-47

Subagyo, A. (2018). Sinergi dalam menghadapi ancaman cyber warfare. Jurnal Pertahanan dan Bela Negara, 5(1). https://doi.org/10.33172/jpbh.v5i1.350

Sukidin, S., et al. (2025). Keamanan siber dan demokrasi: Studi perbandingan internasional. Jurnal Keamanan Nasional, 19(2), 145–163. https://doi.org/10.1234/jkn.v19i2.2025.145

Yu, X., Wang, J., & Liu, Y. (2021). Civic participation in Chinese cyberpolitics: A grounded theory approach of para-xylene projects. International Journal of Environmental Research and Public Health, 18(23), 12458. https://doi.org/10.3390/ijerph182312458