Research Article

Received: 3 March 2024 / Accepted: 30 August 2024 / Published: 05 September 2024

Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity

Mansur Juned[1]

Ali Martin[2*]

Nugraha Pratama[3]

[1]University Pendidikan Nasional Veteran,
Jl. Rs. Fatmawati, Pondok Labu, Jakarta Selatan,
DKI Jakarta, 12450, Indonesia
[2]University Wahid Hasyim, Jl. Menoreh Tengah X No.22, Sampangan,
Kec. Gajahmungkur, Kota Semarang, Jawa Tengah 50232, Indonesia
[3]University Padjadjaran, Jl. Raya Bandung Sumedang KM.21, Hegarmanah,
Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, Indonesia
**Corresponding Author*

DOI: https://doi.org/10.36941/ajis-2024-0171

Abstract

The 2022 cyberattack from the hacktivist Bjorka in Indonesia is an example of evolution in how civil society expresses their interest in the scope of cyberactivism as an essential foundation to cyberdemocracy as the result of the advancement of ICT, rapid growth of internet users, and multi-sectors digitalization. As the trend to use hacktivism as an extreme method of cyberactivism begins to emerge in Indonesia, an essential question arises of how cyberactivism in Indonesia evolved into hacktivism and how it creates problematic relations to cybersecurity and, on the broader term, cyber sovereignty in Indonesia. We investigate the question by conducting a case study exploring information regarding Bjorka hacktivism, the evolution of cyberactivism in Indonesia, government regulation, and so forth through literature studies. The results suggest that Bjorka is the new chapter of cyberactivism in Indonesia that evolves in line with the advancement of ICT, the growth of internet users, and digitalization. It also represents a complex juxtaposed position between cyberdemocracy and cybersecurity.

Keywords: *Indonesia, cyberdemocracy, hacktivism, cybersecurity, cybersovereignty*

1. Introduction

The Bjorka case in Indonesia recently reflects the debate over hacktivism as the ultimate form of cyberdemocracy, security concerns over hacking activities, and the complexity of the public responses to the attack. The attack that began in mid-2022 began with the leak of data from one of the major cellular providers in the deep web forum spread by an anonymous hacker(s) called Bjorka before escalating to more critical data leaks, including registration number, the president's correspondence notes, and data of the famous murder of human rights activist, Munir (Kompas, 2022b; Liputan6, 2022). Furthermore, the attack also generated conflicting statements between the government, which condemned this action as a threat to the nation's cybersecurity, and Bjorka, who perceives the action as an act of hacktivism that escalated into a massive debate in society regarding the case (Nurdiyansyah, 2022; Pramana & Ramdhani, 2023). Some people support the action of Bjorka as an extreme way to criticize the government; others condemn the attack as it puts the private data of the citizens of Indonesia at risk, while others did not pay attention to the issue (Kurniawan & Maujuhan Syah, 2022; Nurdiyansyah, 2022).

Regardless of the claim from both sides, hacking with political motives is relatively complex to be precisely calculated as it is often diffused with other motives such as to gain ransom, popularity, cyberwar, competition, and so forth. However, based on the existing data from Statista (2022), by 2021, there were around 5.5 billion cyberattacks worldwide, while Desjardins (2018) assumed that 24% of total cyberattacks were based on political motives, especially leaking sensitive data, hacking government websites and so forth. However, it is also possible that multiple motives can generate an attack itself (Chng et al., 2022). While determining the main motive of the so-called hacktivist attack is complex, the public recognition of the visible politically motivated cyberattack generates another complexion regarding public responses.

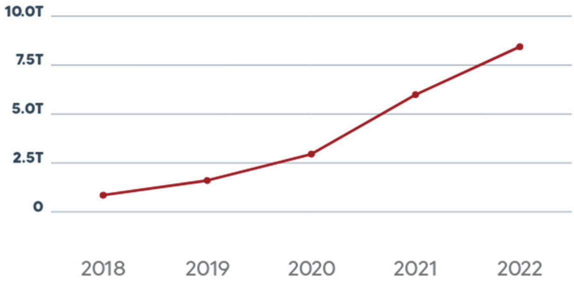

Figure 1. The annual cost of cybercrime trend (Statista, 2022)

The phenomena of hacktivism cannot be separated from the robust growth of internet users and the advancement of ICT that has generated more possible interactions in cyberspace between those asymmetric actors (Adams & Albakajai, 2016; Choucri, 2012; Herrera, 2008; Juned et al., 2022). In the sociopolitical dimensions, more actors involved generate more dynamic interactions between actors in forms and quantity in cyberspace, which also affects the physical interactions in which the term cyberdemocracy emerged (Gerbaudo, 2017; Goby, 2003). Therefore, as cyberspace offers leverage to non-state actors, it also allows asymmetric anarchical relations between actors who try to use the virtual space for their interests, including cyberactivism from civil society, which is the most extreme form in hacktivism (Karatzogianni, 2015; Pratama, 2016). The number of participants and the manifestation of cyberactivism were advancing rapidly as more engagement from the digital migrants, the growing digital natives, and the birth of social media made the political discussion in cyberspace no longer limited (Hennefer, 2013). By 2021, internet users will have reached 4.8 billion people from 7.87 billion people worldwide, and 93% of those internet users will have at least one social media account (Kemp, 2022). Similarly, Anderson et al. (2018) noted that 53% of U.S. internet users engage in political action.

As people's engagement with cyberspace has rapidly increased since the 2000s, the issue of hacktivism, which has existed previously, has arisen as one of the most controversial topics in cybersecurity and cyberactivism (Gerbaudo, 2012). Cybersecurity that has the intention to secure the network from any threats regardless of the intention will be directly challenged by the hacktivism perspective that uses cyber-attacks to gain private data, top secret government documents, or solely to demonstrate political dissatisfaction to governments/corporations by changing the appearances of their websites or applications. Furthermore, these forms of cyberactivism, as well as cyberactivism in general, are perceived as a potential threat to the state actors both for political threats towards the existing regimes, such as in the Arab Spring, as well as to generating polarization in the society that leads to violence as it happened in the Capitol Hill 2021 which the goal is to spread information to provoke people and form of hacktivism in the cases of Anonymous and Wikileaks (Bickerton & Accetti, 2021; Gerbaudo, 2012; Roberts, 2022).

We perceive the Bjorka attack in Indonesia as essential to discuss for its recentness, its relations to the global trend of cyber activism, and its impacts. We argue that the Bjorka case in Indonesia is aligned with the global trend of increasing cyberactivism and hacktivism to articulate critics, arguments, and dissatisfaction, especially towards the government. However, it also cannot be perceived similarly to what happened in the Arab Spring or the peak of the Global Financial Crisis of 2007-2008, as the enhancing digital engagement and polarization in society made the impact more complex and massive. Secondly, the case of Bjorka is challenging to discuss as it happened in a country whose regulations on digital data protection and cybersecurity are still in the early steps. Thirdly, there were different public opinions regarding this issue, with the majority favoring Bjorka's action even though it directly put their data at risk.

Furthermore, we conduct this research using a qualitative approach to grasp the complexity of the case and its complex connection with similar worldwide phenomena. The rationale behind this approach is the abundant data available in the case and the worldwide hacktivism phenomenon due to massive highlights. Therefore, a qualitative approach is suitable for analyzing those secondary data. The research started by gathering details related to Bjorka's attack, including the backgrounds, method of attacks, and reactions from the public and government. However, we also realize that Bjorka is only one among many similar hacktivism worldwide with diverse targets and motives. Therefore, we also focus on how the case of Bjorka has complex connections and is interrelated to other cases elsewhere.

2. Literature Review

Cyberactivism, as the large house for hacktivism, is a complex concept juxtaposed with many concepts related to the intertwined aspect between technological advancement and socio-political conditions. In this regard, we identify that cyberactivism is closely related to cyberdemocracy as the background for the diverse forms of activism and interests articulation in cyberspace, including hacktivism. However, hacktivism, as an extreme form of cyberactivism, has a different dimension as it directly impacts cybersecurity. In this regard, the Bjorka attacks pose threats not only to the state but also to the people. Therefore, the theoretical framework for understanding this case should be incorporated by discussing cyberdemocracy and cybersecurity to enrich the concept of cyberactivism in the context of the Bjorka case.

One of the most significant impacts of ICT advancement is how it allows people to interact with each other to fulfill their interests asymmetrically (Gerbaudo, 2017). In the early era of cyberspace, scholars argued that virtual space would not only change the way people interact but also be optimistic about how it would empower democratization (Fung et al., 2013; Habermas et al., 2001; Kaczmarczyk, 2010, 2012; Norris, 2003). However, the power dynamics within cyberspace, the digital gap, security, and other factors have created another level of complexity in the cyberdemocracy. This leads to the more fundamental question, "Should cyberspace be the space of complete freedom?". The question is not only in the debate of global major powers but also the scholars as reflected in the thought of digital fragmentation by Habermas (Chambers, 2023), the plebiscite democracy of Gerbaudo (2022), and technopopulism (Bickerton & Accetti, 2021) in contrast to the more optimistic perspective of Kaczmarczyk (2012) about cyberdemocracy or synthesis between threats and opportunity of cyberdemocracy in Karagiannopoulos (2018).

Freedom in cyberspace is a fundamental pillar of cyberdemocracy as it allows information to flow across political, geographical, and time boundaries to empower open (Barlow, 1996; Cohen, 2014; Karagiannopoulos, 2018). However, we argue that allowing cyberspace to be completely free and unregulated also attracts vulnerability exploitation to many stakeholders manifested in diverse regulations to secure aspects of cyberspace. Juned et al. (2022) argues that the necessity for regulations in cyberspace emerged into two contrasting arguments promoted by two major powers: freedom of cyberspace from the U.S. and China's more authoritarian restricted cyber sovereignty. This condition leads to a complex dilemma for most governments in providing the most suitable cyberspace policies to balance cybersecurity and freedom of cyberspace and the external pressure from global political powerhouses regarding their domestic condition.

Regardless of the characteristics and necessities for cyberspace regulation, the imposed degree of limitation also attracts resistance from many cyberactivists, including one of the earliest, John Perry Barlow (1996). Cyberspace was considered an alternative space for resistance, and government regulations would eliminate the leverage once the cyberactivists had it (Gerbaudo, 2017; Juned et al., 2022). The resistance towards restrictions is also growing in line with the efforts of governments to regulate virtual space, mainly but not limited to autocratic governments (Gerbaudo, 2017, 2018, 2022; Yang, 2016). The resistance is shifting towards a more negotiable direction between restriction and freedom in cyberspace. Hacktivism intertwines between paradoxical arguments of cyberspace, as Romagna and Leukfeldt (2023) argue that the most common motive of hacktivism is a moral violation by the authorities, while cyberspace provides leverage to overcome limited physical resources in the resistance movements.

Therefore, we construct a theoretical framework based on cyberactivism as the actual topic of the research. However, the theoretical inquiry suggests that the concept of cyberdemocracy and cybersecurity should also strengthen the complex impact of cyberactivism in this case. In this regard, we perceive cyberactivism as a pillar of cyberdemocracy that allows dynamic asymmetric interaction. However, hacktivism, as the extreme type of cyberactivism, becomes a threat not only to cybersecurity in terms of national security but also to people's security in the context of this paper. Furthermore, it also impacts cyberdemocracy by becoming an essential issue that is widely debated in cyberspace as people segregated to protect their own data security or hacktivism that allowed them to know the data security weakness provided by the government.

3. Research Method

We use a qualitative approach to conduct this research to gather and analyze diverse data types from various sources (Creswell & Creswell, 2023). Precise, we use case study analysis in our investigation of Bjorka's cyberattack in Indonesia in 2022 as we acknowledge that even though the use of hacktivism as a form of cyberactivism is a common phenomenon, each case has its uniqueness depending on the main motives, condition, and backgrounds. This research is designed to investigate Bjorka's cyberattack as a form of hacktivism and capture its relations with cybersecurity for the people and the government. To gain complete insight into the phenomena, we analyze the topic by studying the details chronologically, including its complex related factors: socio-political, digital literature of the people, cyber regulation, receptions, and internet penetration in Indonesia. While we acknowledge that the background in Indonesia differs from other countries, we also compare the phenomena with similar phenomena in different countries to deepen our understanding of Bjorka's cyberattack.

This research uses mainly digital data as the primary and secondary sources. We use trend analysis, government releases, and regulations as the primary data. Furthermore, we use news from diverse sources, third-party trend analysis, and academic documents highlighting similar cases to the research's secondary data. As the perspective of the data sources can be different in perceiving hacktivism, we carefully contrasted those differences to gather complete information to deepen our analysis by using literature selection criteria which include: relevance to the study, recentness, ensuring the validity of the data and literature, and since the topic is controversial, we also categorize the data by those key perspectives.

Furthermore, we employed thematic analysis to review the chosen literature, identifying major themes concerning cyberactivism, cybersecurity, cyberdemocracy, and Bjorka's impact in Indonesia. A comparative approach was then used to examine various scholarly perspectives on hacktivism's role in influencing cybersecurity policies, public discourse, and cyberdemocracy in general. We also employed our observation to measure the public and scholarly sentiment of Bjorka by employing the digital inquiry in X (formerly Twitter) and Researchgate. By analyzing areas of agreement and disagreement in the literature, the study concluded Bjorka's specific effects on Indonesia's cyber landscape, including theoretical and practical implications such as shifts in cybersecurity measures, public opinion, and government responses. This method allowed for a thorough examination of existing research, providing a solid basis for understanding Bjorka's significance within the broader context of Indonesian cyberactivism, cyberdemocracy, and cybersecurity.

We also acknowledge several ethical considerations related to the topic of this research. Therefore, this study adheres to strict ethical standards, particularly concerning data privacy and research integrity. All data regarding Bjorka's hacktivism are sourced from publicly available materials, ensuring that no unauthorized or sensitive information is disclosed. Ethical dilemmas inherent to hacktivism are addressed with a neutral stance, focusing on analysis rather than endorsement of illegal activities nor to corner the cyberactivism movement. The study also ensures responsible scholarship by carefully considering the broader societal implications of cyberactivism without discrediting, sensationalizing or glamorizing illegal actions. These ethical safeguards maintain the integrity and objectivity of the research.

4. Result and Analysis

4.1 The Case of Bjorka in Indonesia

Bjorka's attack began with malware to leak the secured data of both corporates and state agencies and put them in auction in the deep web forums that recently happened to the users of the biggest tech startup in Indonesia (Tempo, 2022). By the mid of 2022, Bjorka launched a series of cyberattacks started by the data leaking of users of the most significant cellular and mobile internet provider that continued into the data leaking of users' mobile phone registration and put them for sale in the deep web forum (Kontan, 2022). Bjorka continued his/her actions by leaking more private, government-classified data to the deep web while also amplifying his/her popularity and intention via social media (Liputan6, 2022). Despite the provider's claim of denial, the validity of a small percentage of data was confirmed by the Ministry of Communication and Information of the Republic of Indonesia (Kompas, 2022a; Suara Surabaya, 2022).

The government condemned the attack and perceived it as civil disobedience and a threat to Indonesia's domestic cybersecurity. In response, Bjorka, through the social media account, threatened to leak even more significant numbers and quality data, followed by the leak of the citizen registration number and the personal data of the government officials while calling them stupid and corrupt (Septiani, 2022). The attack then became public attention and generated debate among the Indonesian people, especially in social media, mainly Twitter, regarding the action and whether it was a threat or heroic hacktivism as there is public concern regarding the delayed personal data protection law (Nurdiyansyah, 2022; Pramana & Ramdhani, 2023).

Nevertheless, Bjorka's hacktivism continues regardless of Indonesia's government's effort to hunt Bjorka, condemnation, and diverse public reactions (Tempo, 2022). The government's effort to hunt Bjorka failed as they only found the hacker and also used subordinates to conduct the actions and also as decoys. The effort to suppress people's unrest by blocking Bjorka's social media account failed as the account continuously changed to outsmart the government's effort. The failure led to more civil unrest as the government failed to protect citizens' data, making Bjorka more prevalent among people (Nurdiyansyah, 2022). In response, the government fastened legislation on personal data protection law and finally legalized it in the last quarter of 2022 to stop the unrest and provide more resources to arrest Bjorka (CNBC Indonesia, 2022). However, even after the personal data protection law legalization, Bjorka's action continued until at least today (February 2024) in less intensity, and his identity of him/her remains unsolved.

4.2 *Evolving Cyberactivism and Hacktivism in Indonesia*

Bjorka is not the first time Indonesia has had a widely acknowledged cyberactivism since the nation already has several notable cyberactivism as it also happened in populism-fueled identity politics campaign in the 2019 election, Pancasila versus Khilafah, and Gejayan Memanggil and so forth (LP3ES, 2021; Rahmawan et al., 2020; Zakaria, 2023). In more specific terms of hacktivism, there were also several notable types of hacktivism previously that both targeted governments and corporations, such as the cyberattack of Komisi Pemilihan Umum (National Election Commission) in 2004 and the attack of Telkomsel, a state-owned telecommunication service company, in 2017 and so forth even though all those actions did not generate impacts as massive as Bjorka (Kompas, 2017; Tempo, 2004).

The trend of using cyberspace as a medium for political activities in Indonesia is evolving symmetrically to advance internet access. The data from Statista (2022) and the Indonesian Central Agency of Statistics (BPS) suggest that Internet penetration in households and at individual levels in Indonesia has been at a steady rate of around 4 percent annually in the last 5 years. The intercourse of cyberspace and politics in Indonesia can be traced to the fall of the Soeharto regime in the late 1990s, in which cyberspace acted as the non-controlled space that allowed the activists to spread information without government's censor as well as an organized physical, political movement among young intellectuals similar to Arab Springs movement (Gerbaudo, 2012; Lim, 2003, 2006).

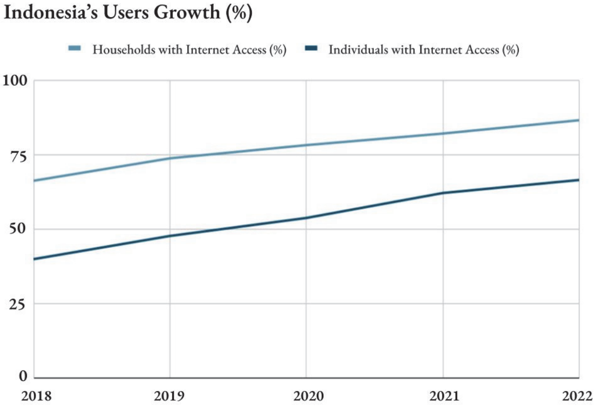

Figure 2. Indonesia's internet users growth

The fall of the authoritarian Soeharto regime provided more supportive regulation towards advancing internet technology and its use in political discussion with the published Law No. 36 1999 about ISP rights and obligations (Indonesian Government, 1999). The law provides a legal basis for internet technology advancement that facilitates more excellent internet users' growth to support civil liberties in the country's democratization process in the early post-Soeharto era. However, the regulations also allow the government to monitor and regulate the internet to prevent and react to malicious activities in cyberspace, including cyberattacks and forbidden information dissemination.

In the early 2000s, cyberactivism was only implemented in a limited scope but had a powerful impact on civil activism in the transition period (Lim, 2006). However, the growing number of internet users due to technological advancements has also generated different methods of cyberactivism. One of the most notable ones is the deface attack on the KPU (election commission) website to protest against its large budget allocation (Tempo, 2004). The introduction of social media such as Friendster and later Facebook between 2004 and 2005 opened a new era for cyberactivism in Indonesia, catalyzing a growing number of internet users and some cyberactivists (Dewantara & Widhyharto, 2016). The existence of social media also allows people not only to express their interests via social media but also promote the links to other websites that provide other room for activism from chatrooms, petitions, polling, blog posts, and so forth (Khamis, 2013; Nofrima et al., 2020; Sandoval-Almazan & Ramon Gil-Garcia, 2014).

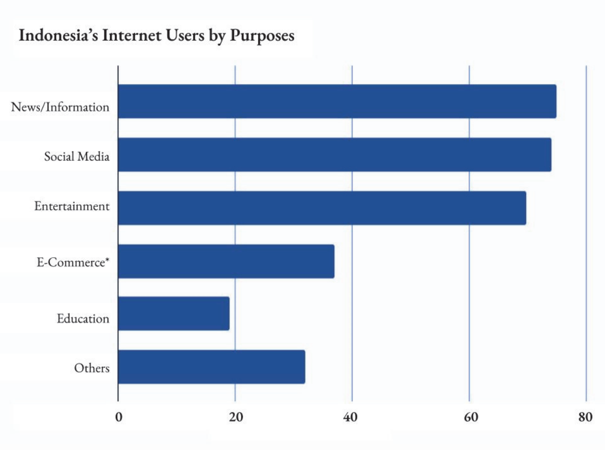

Figure 3. The use of the Internet in Indonesia.

We argue that the rise of social media popularity and its growing users in Indonesia, especially after 2010, as well as the centralized cross-platform instant messenger, generates significant changes in cyberspace and cyberactivism in more specific terms. It acts as a virtual common space for people with diverse backgrounds and intentions to acknowledge the diversity of cyberspace via sharing information. Therefore, it allows "secluded information that previously was only a concern for limited people to be amplified and acknowledged by the public virtually. Cyberactivism increased significantly in people involved, types, and issues covered, making cyberspace more effective for conducting cyber campaigns and coordinating physical movement. Cyberspace has become the space for people to discuss and criticize the government domestically and show nationalism or cyber nationalism through social media posting, articles, hate speech, and event launch cyberattacks towards other countries (Cyberthreat, 2019).

The result of the above condition is well represented in Indonesia's diverse forms of cyberactivism from 2010 until now. During this period, social media became the primary media for cyberactivism, primarily through Facebook and Twitter, as is reflected by countless movements in the form of diverse hashtags. One of the most obvious is how social media became the primary tool for the supporters of the 2019 Indonesia presidential election to express their interests and concerns in the form of positive campaigns, negative campaigns, and even black campaigns (Gunia, 2019; Hui, 2020; Irawanto, 2019). Similarly, the trend of petitioning online is also rising significantly, covering diverse issues from animal rights activism on the issue of dog meat consumption to the religion-based political movement in the case of Basuki Tjahaya Purnama's removal as the governor of Jakarta in 2016 (Hui, 2020; Irawanto, 2019). Nonetheless, the case of hacktivism has also arisen as the new popular tool to express civil resistance towards restricting government policies in cyberspace. Besides the mentioned example, many issues and forms of activism gained wide public attention in this period due to social media's ability to amplify the recognition from the people.

However, the increasing use of social media also attracts adverse effects and new types of threats from cyberattacks, cyberbullying, and hoaxes with greater magnitudes and impacts. In response, the government of Indonesia imposed more restrictive regulations about electronic information and transactions in Law No. 16 2016 to replace Law No. 11 2008 (Indonesian Government, 2008, 2016). Even though the updated regulations were necessary to respond to the dynamics within cyberspace, they mainly received adverse reactions from the people who perceived that the law was an effort from the government to take control of cyberspace and silence the unwanted voices from the people.

4.3 Cyberactivism and Cybersecurity Paradox

The case of Bjorka also displays classic debates regarding hacktivism from the perspective of cyberactivism and cybersecurity. In the classic typology of cyberactivism, hacktivism can be considered one of the most extreme methods of cyberactivism by intentionally conducting cyberattacks in diverse forms from DDoS, website defaces, confidential data leaking, and so forth in regards to political motives (Karagiannopoulos, 2018; Karatzogianni, 2015; Sauter, 2014). Even though hacktivism shares similarities with other forms of cyberactivism that use cyberspace as the movement arena that gives them leverage to push changes in society and political struggle and pressure on corporations and governance to accommodate civil interests, the extreme methods employed in hacktivism also latent threats in the perspective of cybersecurity. While the methods themselves can be categorized as cybercrime in most national laws regarding cyberspace, using those methods as acts of political struggle in the context of hacktivism generates a rising trend of cyberattacks for political motives.

However, hacktivism can also be perceived differently in the perspective of cyberactivism based on the argument of freedom in cyberspace. The existing hacktivism is a normal phenomenon when other forms of cyberactivism have proven less effective in generating socio-political changes in both the elites and society. In this regard, the rise of hacktivism is a consequence of the freedom to express interest in cyberspace being silenced by regulations that consider those actions unlawful acts of cybercrime or being ignored by the people. Furthermore, the categorization of hacktivist acts as cybercrime rather than the voice of the people essentially is an act of neglecting the principle of freedom on the internet because the authority is more focused on securing its power rather than acknowledging the concern behind the attack by using the more repressive law of cybersecurity that in this case is reflected in the message of Bjorka regarding rights for the public to access the "truth" behind the controversial events as well government's inability to protect the data of the people.

Cyberactivism is an essential element of cyberdemocracy, as cyberspace's freedom of speech should also be protected as the foundation of cyberdemocracy beyond procedural forms. With the law protecting freedom of expression in cyberspace, cyberdemocracy will be in procedural discourse. However, while the essence of cyberdemocracy is to allow the essential discourse of common issues in the virtual public space to generate input for the decision-making process, the implementation of cyberdemocracy, in reality, has different characteristics that must be addressed. The most essential unique characteristic of cyberdemocracy is cyberspace, which differs significantly from the physical ones, especially regarding power struggles. Gerbaudo (2017) argues that at the beginning of unregulated cyberspace, people used virtual space to conduct struggle against governments and corporations more effectively in contrast to the physical ones as there were less restrictive regulations at the time, making it almost utopian space democracy finally blossoming. This condition creates an asymmetric power struggle in cyberspace between governments, corporations, and people with amplified complexity, making consensus more difficult to achieve fully.

Arab Springs, many cases of hacktivism, including Bjorka, and many forms of cyberactivism suggest that it is difficult to achieve such a consensus, and the involved parties try to exercise their power to ensure the fulfillment of their interest regardless of the others. However, the struggle becomes problematic as it relates to political aspects and other aspects that generate more significant consequences for every action the parties take. It is not surprising in the end that cyber or digital securitization becomes imminent as diverse regulations of cyberspace reflect it to ensure cybersecurity that while it is secure in the interests of several people, it generates negative responses from others, such as in ITE law in Indonesia or Twitter policy during 2020 US Presidential election. However, the consensus of how cyberspace should be, at least in the aspect of cybersecurity itself, is a complex milestone as the still growing cyberspace, digital divide, and different perspectives on perceiving cyberspace itself, notably in the discourse of freedom on cyberspace and cybersovereignty that can be different between countries and societies.

Bjorka hacktivism in Indonesia can only be perceived from a political perspective regarding Indonesia's economic and social aspects. As a middle-income country's incoming demographic boom in 2045, the Indonesian government intensively encourages a higher rate of digital adaptation through massive digital transformation in every aspect to boost the country's economic performance. This condition increases digital engagement among the people even though the level of readiness of the people remains in question, reflected in the low digital literation, less civil digital interaction, unequal access to high-speed internet due to unequal income, and so forth (Amanta, 2022; Juned & Pratama, 2023). Combined with the less effective regulation in cyberspace, those factors induce more chances for cyberattacks and other cyber-related socio-political and economic threats.

We argue that in the case of Indonesia, the trajectory of digital penetration, the use of social media, cyberdemocracy trends, policy readiness, and grassroots political understanding generate a challenging future for Indonesia in balancing cybersecurity and cyberdemocracy. The case of Bjorka reflects the contrasting perspectives among people regarding how they perceive cyberdemocracy in the form of free acts in cyberspace and cybersecurity. Furthermore, the government's regulations seem inadequate to respond to existing dynamics or the normative foundation based on a hybrid perspective of data sovereignty and cyber sovereignty, widely acknowledged and accepted among the people (Juned & Pratama, 2023). In addition, Indonesia should also consider the rivalry between the two giants of the US and China that extends to cyberspace beyond geopolitics (Sudirman et al., 2019). Moreover, this existing condition also creates a consensus regarding the paradox.

5. Conclusion

Bjorka's cyber-attack in Indonesia is essential in the existing discourse between cyberactivism and cybersecurity. Domestically, this case is an essential milestone in the chronology of cyberdemocracy in Indonesia as it used a new method of attack and the first time such hacktivism gained massive public attention. The combination of large numbers of internet users, mainly social media users, the digitalized Indonesian society during the pandemic, momentum regarding personal data protection, and relatively open cyberspace contribute to this condition. However, we argue that one of the most pivotal uniqueness of Bjorka's case is the hacker's ability to draw public attention from the case through a series of statements in his/her social media account even after the main concern resided and used the data, he/she hacked for his/her interest by auctioned it in the deep web. Furthermore, even though the general perception regarding Bjorka is negative, the small number of positive opinions regarding him/her suggests that the hacker has become a cult hero and/or generated pro-hacktivism among his/her supporters, which adds a new layer of complexity between cybersecurity, and cyberdemocracy paradox.

Bjorka's attack also suggests the latest manifestation of the discourse of cyberactivism and cybersecurity perspectives regarding hacktivism. The term hacktivism has become the focus of discourse between cybersecurity, which perceives it as a threat to cybersecurity in general, and the perspective of cyberactivism that puts hacktivism as its most extreme form when other forms failed to achieve its goals as the result of restrictions towards the actual establishment of cyberdemocracy.

Reflecting on the Bjorka case, the paradox is also influenced by the number of internet users, the related policies, social media, and the normative foundation of a nation's perspective on cyberspace.

Furthermore, the case of Bjorka also highlights the urgency of adequate data protection mechanisms from the government, such as the implementation of the Personal Data Protection Act, which was being exploited by Bjorka. In this regard, we argue that the Bjorka case suggests that the roots of the cyber vulnerability in Indonesia are deeper than inadequate law enforcement or mechanism, but also the significant digital gap and digital literacy among the people, government officials and law enforcers. This condition leads to a lack of digital awareness at both government and individual levels. This condition leads to the perspective that digital data protection is less essential to be put under the spotlight of the general digital-related policies manifested in inadequate data protection mechanisms and low awareness from people regarding their data security. Furthermore, the combination of inadequate data protection mechanisms, low digital awareness, the restrictive ITE law, and the late democratization process in Indonesia generate digital segregation and a relatively segregated and exclusive form of cyberdemocracy, characterizes by excessive attention towards virality instead of validity.

We argue that adequate data protection mechanisms should be made a national priority, considering the attack of Bjorka and its aftermath. It is essential to ensure data protection for the government and the people and limit further, more severe hacktivism. We argue that such a limitation is essential to guard the growing importance of cyberactivism and cyberdemocracy in Indonesia. Furthermore, we also suggest that improving digital literacy to raise digital awareness is essential, as we believe the foundation of cybersecurity is the awareness of the digital environment, including data protection.

References

Adams, J., & Albakajai, M. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, *4*(6), Article 6. https://doi.org/10.17265/2328-2185/2016.06.003

Amanta, F. (2022, July 6). *Unpacking Indonesia's Digital Accessibility*. https://www.cips-indonesia.org/post/opinion-unpacking-indonesia-s-digital-accessibility

Anderson, M., Toor, S., Olmstead, K., Rainie, L., & Smith, A. (2018, July 11). *Activism in the Social Media Age*. Pew Research Center. https://www.pewresearch.org/internet/2018/07/11/activism-in-the-social-media-age/

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Bickerton, C. J., & Accetti, C. I. (2021). *Technopopulism: The New Logic of Democratic Politics* (1st ed.). Oxford University Press. https://doi.org/10.1093/oso/9780198807766.001.0001

Chambers, S. (2023). Deliberative democracy and the digital public sphere: Asymmetrical fragmentation as a political not a technological problem. *Constellations*, *30*(1), Article 1. https://doi.org/10.1111/1467-8675.12662

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press; JSTOR. http://www.jstor.org/stable/j.ctt5hhkrs

CNBC Indonesia. (2022, September 29). *UU PDP Disahkan, Hacker Bjorka Justru Menghilang*. https://www.cnbcindonesia.com/tech/20220929083913-37-375809/uu-pdp-disahkan-hacker-bjorka-justru-menghilang

Cohen, E. D. (2014). Democracy in Cyberspace. In E. D. Cohen, *Technology of Oppression* (pp. 85–98). Palgrave Macmillan US. https://doi.org/10.1057/9781137408211_6

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (Sixth edition). SAGE.

Cyberthreat. (2019, Desember). *Sejumlah Insiden Hacktivism di Indonesia Antara 2017-2019*. https://cyberthreat.id/read/4389/Sejumlah-Insiden-Hacktivism-di-Indonesia-Antara-2017-2019

Desjardins, J. (2018, January 3). *Why Hackers Hack: Motives Behind Cyberattacks*. https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/

Dewantara, R. W., & Widhyharto, D. S. (2016). Aktivisme dan Kesukarelawanan dalam Media Sosial Komunitas Kaum Muda Yogyakarta. *Jurnal Ilmu Sosial Dan Ilmu Politik*, *19*(1), Article 1. https://doi.org/10.22146/jsp.10855

Fung, A., Gilman, H. R., & Shkabatur, J. (2013). Six Models for the Internet + Politics. *International Studies Review*, *15*(1), Article 1. JSTOR.

Gerbaudo, P. (2012). *Tweets and the streets: Social media and contemporary activism*. Pluto Press.

Gerbaudo, P. (2017). From Cyber-Autonomism to Cyber-Populism: An Ideological Analysis of the Evolution of Digital Activism. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *15*(2), 477–489. https://doi.org/10.31269/triplec.v15i2.773

Gerbaudo, P. (2018). *The Digital Party: Political Organisation and Online Democracy*. Pluto Press. https://doi.org/10.2307/j.ctv86dg2g

Gerbaudo, P. (2022). Theorizing Reactive Democracy: The Social Media Public Sphere, Online Crowds, and the Plebiscitary Logic of Online Reactions. *Democratic Theory*, *9*(2), Article 2. https://doi.org/10.3167/dt.2022.090207

Goby, V. (2003). Physical Space and Cyberspace: How Do They Interrelate? A Study of Offline and Online Social Interaction Choice in Singapore. *CyberPsychology & Behavior*, *6*(6), Article 6. https://doi.org/10.1089/109493103322725414

Gunia, A. (2019, April 17). *Social Media Gets a Bad Rap in Elections, But Activists In Indonesia Are Using It to Boost Transparency*. https://time.com/5567287/social-media-indonesia-elections-kawal-pemilu/

Habermas, J., Rehg, W., & Habermas, J. (2001). *Between facts and norms: Contributions to a discourse theory of law and democracy* (1 MIT Press paperback ed., 4. printing). MIT Press.

Hennefer, A. (2013). *Cyberactivism: A generational comparison of digital activism* [University of Nevada, Reno]. http://hdl.handle.net/11714/3252

Herrera, G. L. (2008). Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In *Power and Security in the Information Age* (p. 27). https://www.taylorfrancis.com/chapters/edit/10.4324/9781315601793-4/cyberspace-sovereignty-thoughts-physical-space-digital-space-geoffrey-herrera

Hui, J. Y. (2020). SOCIAL MEDIA AND THE 2019 INDONESIAN ELECTIONS. *Southeast Asian Affairs*, 155–172. JSTOR.

Indonesian Government. (1999). *Law Of The Republic Of Indonesia Number 36 Of 1999 On Telecommunications*.

Indonesian Government. (2008). *Law No.11 2008 about electronic information and transaction*.

Indonesian Government. (2016). *Law No. 16 2016 about electronic information and trasaction*.

Irawanto, B. (2019). *Making It Personal: The Campaign Battle on Social Media in Indonesia's 2019 Presidential Election*. *28*(2019).

Juned, M., Bainus, A., Saripudin, M. H., & Pratama, N. (2022). The dynamics of the USA and China relations in the cyberspace: Struggle for power in a global virtual world in building a global cyber regime. *International Journal of Business and Globalisation*, *30*(3/4), 396. https://doi.org/10.1504/IJBG.2022.123617

Juned, M., & Pratama, N. (2023). Demokrasi siber dan kedaulatan siber di Asia Tenggara dalam membangun Masyarakat Digital ASEAN 2025. In Y. Syukur (Ed.), *ASEAN episentrum pertumbuhan pertumbuhan dunia. Gagasan konstruktif Masyarakat Indonesia* (p. 950). MATA KATA INSPIRASI.

Kaczmarczyk, A. (2010). *Cyberdemocracy: Change of democratic paradigm in the 21st century* (1st ed). Key Pub. House.

Kaczmarczyk, A. (2012). Cyberdemocracy as a Future Product of Political Systems Engineering. *Frontiers in Science*, *1*(1), Article 1. https://doi.org/10.5923/j.fs.20110101.02

Karagiannopoulos, V. (2018). *Living With Hacktivism*. Springer International Publishing. https://doi.org/10.1007/978-3-319-71758-6

Karatzogianni, A. (2015). *Firebrand Waves of Digital Activism 1994–2014*. Palgrave Macmillan UK. https://doi.org/10.1057/9781137317933

Kemp, S. (2022). *Digital 2022: Global Overview Report*. https://datareportal.com/reports/digital-2022-global-overview-report

Khamis, S. (2013). "Cyberactivism" in the Arab Spring: What social media can and cannot do. *International Affairs Forum*, *4*(1), Article 1. https://doi.org/10.1080/23258020.2013.824258

Kompas. (2017). *Begini kronologi peretasan situs menurut dirut Telkomsel*. Kompas.Com. https://tekno.kompas.com/read/2017/04/28/18471727/begini.kronologi.peretasan.situs.menurut.dirut.telkomsel

Kompas. (2022a, February 9). *Data Registrasi SIM Prabayar Diduga Bocor, Kominfo, Dukcapil dan Operator Kompak Mengelak*. Kompas.Com. https://tekno.kompas.com/read/2022/09/02/10000017/data-registrasi-sim-prabayar-diduga-bocor-kominfo-dukcapil-dan-operator-kompak?page=all

Kompas. (2022b, December 9). *Keriuhan Bjorka: Klaim bongkar data pemerintah hingga kasus Munir, tiba-tiba akunnya "menghilang*. https://www.kompas.com/tren/read/2022/09/12/160000965/keriuhan-bjorka--klaim-bongkar-data-pemerintah-hingga-kasus-munir-tiba-tiba?page=all#

Kontan. (2022). *Lagi, Data Pribadi Warga Indonesia Dijual Di Internet, Kini Data Registrasi Kartu Hp*. https://nasional.kontan.co.id/news/lagi-data-pribadi-warga-indonesia-dijual-di-internet-kini-data-registrasi-kartu-hp

Kurniawan, D., & Maujuhan Syah, A. (2022). The Impact of Bjorka Hacker on the Psychology of the Indonesian Society and Government in a Psychological Perspective. *CONSEILS: Jurnal Bimbingan Dan Konseling Islam*, *2*(2), Article 2. https://doi.org/10.55352/bki.v2i2.627

Lim, M. (2003). The Internet, social networks, and reform in Indonesia. In *Contesting media power: Alternative media in a networked world*. PublisherRowman & Littlefield.

Lim, M. (2006). Cyber-Urban Activism and Political Change in Indonesia. *Eastbound*, *1(1): 1-19*. https://www.researchgate.net/publication/267939105_Cyber-Urban_Activism_and_Political_Change_in_Indonesia

Liputan6. (2022). *11 Fakta Hacker Bjorka yang Retas Data Pemerintah Indonesia*. https://www.liputan6.com/citizen6/read/5067854/11-fakta-hacker-bjorka-yang-retas-data-pemerintah-indonesia

LP3ES. (2021, January 15). *Aktivisme Digital, Polisi Siber dan Kemunduran Demokrasi*. https://www.lp3es.or.id/2021/01/15/aktivisme-digital-polisi-siber-dan-kemunduran-demokrasi/

Nofrima, S., Nurmandi, A., Kusuma Dewi, D., & Salahudin, S. (2020). Cyber-activism on the dissemination of #Gejayanmemanggil: Yogyakarta's student movement. *Jurnal Studi Komunikasi (Indonesian Journal of Communications Studies)*, *4*(1), Article 1. https://doi.org/10.25139/jsk.v4i1.2091

Norris, P. (2003). Preaching to the Converted?: Pluralism, Participation and Party Websites. *Party Politics*, *9*(1), Article 1. https://doi.org/10.1177/135406880391003

Nurdiyansyah, M. (2022, September 22). Memaknai Anomali Respons Publik terhadap "Hacker" Bjorka. *Detik.Com*. https://news.detik.com/kolom/d-6306007/memaknai-anomali-respons-publik-terhadap-hacker-bjorka

Pramana, T. A., & Ramdhani, Y. (2023). Sentiment Analysis Tanggapan Masyarakat Tentang Hacker Bjorka Menggunakan Metode SVM. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *6*(1), Article 1. https://doi.org/10.32672/jnkti.v6i1.5583

Pratama, N. (2016). *Dinamika hubungan Amerika Serikat dan Republik Rakyat Tiongkok dalam cyberspace 2010-2015*. Universitas Padjadjaran.

Rahmawan, D., Mahameruaji, J. N., & Janitra, P. A. (2020). Strategi aktivisme digital di Indonesia: Aksesibilitas, visibilitas, popularitas dan ekosistem aktivisme. *Jurnal Manajemen Komunikasi*, *4*(2), Article 2. https://doi.org/10.24198/jmk.v4i2.26522

Roberts, K. M. (2022). Populism and Polarization in Comparative Perspective: Constitutive, Spatial and Institutional Dimensions. *Government and Opposition*, *57*(4), Article 4. https://doi.org/10.1017/gov.2021.14

Romagna, M., & Leukfeldt, R. E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, 1–19. https://doi.org/10.1080/0735648X.2023.2216189

Sandoval-Almazan, R., & Ramon Gil-Garcia, J. (2014). Towards cyberactivism 2.0? Understanding the use of social media and other information technologies for political activism and social movements. *Government Information Quarterly*, *31*(3), Article 3. https://doi.org/10.1016/j.giq.2013.10.016

Sauter, M. (2014). *The coming swarm: DDoS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Academic, an imprint of Bloomsburg Publishing Inc.

Septiani, L. (2022, August 7). *Setelah Sebut Kominfo Bodoh, Hacker Bjorka Jual Jutaan Data Pemilu RI*. Katadata. https://katadata.co.id/desysetyowati/digital/63184bd4bc65e/setelah-sebut-kominfo-bodoh-hacker-bjorka-jual-jutaan-data-pemilu-ri

Statista. (2022). *Internet penetration rate in Indonesia from 2017 to 2020 with forecasts until 2026* [dataset]. https://www.statista.com/statistics/254460/internet-penetration-rate-in-indonesia/

Suara Surabaya. (2022, September 1). *CISSReC: Sampel Data Registrasi Kartu SIM yang Diduga Bocor Valid*. https://www.suarasurabaya.net/kelanakota/2022/cissrec-sampel-data-registrasi-kartu-sim-yang-diduga-bocor-valid/

Sudirman, A., Mooy, J., Maluft, M. F., & Ramadhan, R. A. (2019). Militarising the Natuna Islands for Indonesia's Gunboat Diplomacy. *Central European Journal of International & Security Studies*, *13*(4), Article 4.

Tempo. (2004, December 23). *Penjebol situs KPU divonis 6 bulan penjara*. https://nasional.tempo.co/read/53570/penjebol-situs-kpu-divonis-6-bulan-penjara

Tempo. (2022, September 12). *Sosok Bjorka, Peretas yang Mengacak-acak Sistem Data Indonesia*. https://grafis.tempo.co/read/3087/sosok-bjorka-peretas-yang-mengacak-acak-sistem-data-indonesia

Yang, G. (2016). Activism. In B. Peters (Ed.), *Digital keywords: A vocabulary of information society and culture*. Princeton University Press.

Zakaria, D. (2023). Praktik Kewargaan Digital Sebagai Edukasi Publik: Kajian Aktivisme Digital Di Indonesia. *Jurnal Komunikasi Profesional*, *6*(6), Article 6. https://doi.org/10.25139/jkp.v6i6.5293