www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Bjorka: A Cyber Crime Phenomenon Which Gets Support from the Community Using Analysis of Criminological Perspective

Hegar Gagah Anantaka[1], Eva Achjani Zulfa[2], Surya Nita[3]
[1,2,3]Universitas Indonesia
hegargagah@gmail.com

Abstract

Indonesia is experiencing several cybercrimes mostly in the form of online fraud and extortion, phishing and hacking. Since the Covid-19 pandemic hit, Indonesia has been faced with several hacking cases containing Indonesian people's personal data where this data was traded illegally on internet sites. One case that has received a lot of attention from the public in a longer period of time than usual is the hacking case by a hacker named Bjorka. However, the cyber crime case in the form of hacking and doxing that was carried out by Bjorka actually received support from the majority of Indonesian people rather than criticism. The criticism of the Indonesian people was actually directed at the government and this criticism was getting stronger driven by the hacktivism carried out by Bjorka. The research was compiled with the aim of knowing the background and factors that made the Bjorka cybercrime case different and popular among the public and thus gained support through a criminological perspective. The method used to compile this research is a qualitative method with literature study. This paper concludes that according to the RAT (Routine Activity Theory) Bjorka's cybercrime has succeeded in attracting the attention of the Indonesian people because Bjorka has the right motivation as an actor and target of victims, besides that government agencies are unable to maintain national cyber security with solidity. This study also has the conclusion that Bjorka received public support through his hacktivism on social media.

Keywords
Cybercrime; hacktivism; Indonesia; routine activity theory

I. Introduction

Yury Fedotov as the former Executive Director of UNODC (United Nations Office on Drugs and Crime) stated (2017) regarding how technology has changed how crime is seen and perceived by the world because technology has not increased crime in the past, most of which occurred without the help of technology. When technology meets globalization, which has made almost all of humanity benefit from technology, it is undeniable that these benefits are also shared by criminals. They use crime as a platform to commit crimes because technology helps to expand their reach in committing crimes.

In criminology, criminal activity that is detrimental and unlawful is carried out using a technology platform known as action mala prohibita. Hagan and Daigle (2018: 42) explain that simply mala prohibita is a crime that is considered a crime because this action is something that is prohibited by law both at the national and international levels. Over the past decade, technological developments have really been at the peak of their development, especially with the emergence of the Covid-19 pandemic, which had forced everyone to be in their respective homes, becoming a vessel for people who previously did not use technology too much to rely heavily on technology. .

DOI: https://doi.org/10.33258/birci.v6i2.7600

Pasculli (2020: 49) provides a definition of cybercrime that the category played as crime is information and communication used in technology. So in this case, when computer technology that can provide information and communication becomes a target, or becomes a tool, so that it has a role in committing crimes, then all of these things can be categorized as cyber crimes (Pasculli, 2020, p. 49). In sociology, there are two types of crimes, namely deviance and crime.

Cybercrime can lead to both of these things (Song, 2018, pp. 11-12), because to see cybercrimes that are of the deviant type there are cultural, moral, and historical aspects that must be considered. As every country is different in terms of cultural, moral, and historical aspects with other countries. Meanwhile, to look at cybercrime with the type of criminal act, it can be seen through whether the action resulted in something that endangered or damaged the integrity, privacy, freedom, and interests of other people.

Indonesia itself has a BSSN (State Crypto and Cyber Agency) which was formed in 2017 and operates with the main function of protecting everything related to information and communication in Indonesia as an institution which is a fusion of the National Crypto Agency, then Directorate of Information Security, Directorate General Informatics Applications, and the Ministry of Communication and Information (BSSN, 2022). Regardless of its establishment more than five years ago, Indonesian cybersecurity is still frequently subject to cyberattacks and has even developed into cybercrimes that cause harm to individuals, groups or society, such as cases of hacking and data theft that have occurred in the last two years in during the Covid-19 pandemic.

During the last two years in the era of the Covid-19 pandemic, Indonesia has experienced several cases of cybercrime that have shaken society, starting in 2020 with the Tokopedia case, which experienced massive data theft, with approximately 91 million personal data being sold by criminals. cyber on black market sites (Franedya, 2020). Then in 2021 Indonesia was again shocked by a similar hacking case that attacked the Indonesian Attorney General's Office where the stolen and suspected data were the data of the Indonesian Attorney's Office employees (CNN Indonesia, 2021). The hacking cases that shocked the community did not end in 2020 and 2021, but it seems that Indonesia has again experienced cybercrime by hackers whose names are known to almost all of Indonesia, namely Bjorka, who made his public debut after selling

Indihome data, SIM Card registration, to personal data from the KPU (Dewi, 2022). Apart from these hacking and data theft cases, Indonesia is also filled with public complaints about cyber crimes related to extortion, phishing, data exploitation, etc.

Among the many cybercrime cases, the Bjorka cybercrime case received the most attention from the Indonesian people. Apart from hacking and data theft, Bjorka also often appears on social media for several social media interactions that make people even more intrigued by these hackers. Bjorka also leaked the data of several state officials several times at the demands of the Indonesian people who wanted Bjorka to demonstrate his abilities as a hacker in the form of a challenge. The challenges presented by the community made Bjorka even more eager to show his abilities by inserting opinions in the form of protests against the Indonesian government several times on his social media.

In the cybercrime phenomenon and with previous cases that have similarity, Bjorka's case received a more different response because of the way and intent of his crime which made society not only demand him to commit crimes with good reasons, but also many people support Bjorka in in his crime. This is because many of Bjorka's cyber crime cases are related to the Indonesian government and several officials who are considered not to have carried out their duties and obligations to govern society properly.

If before Bjorka there had been two cases in 2020 and 2021 which also linked several hackers and shocked Indonesia, Bjorka showed the difference by not just selling hacked data. But showed he has plenty of criticism of the government by posting a few tweets on social media about his viewpoint on the injustice of the Indonesian government. The background that supports his motivation to commit cyber crimes is what makes many people support his actions. Thus, this research was formed to find out how the phenomenon of the Bjorka cybercrime case, which should have received criticism, actually received a lot of support from the public by analyzing Bjorka through a criminological perspective.

To answer this question, researchers will begin by writing a descriptive explanation of cybercrime in criminology, then proceed with an analysis of the phenomenon of the Bjorka cybercrime case from a criminological perspective. The following sub-chapters will discuss an analysis of the role of the Indonesian government in responding, handling, and preventing cyber crime cases such as Bjorka's to strengthen and develop Indonesia's cyber security so that it becomes more robust.

1.1 Formulation of the problem

Ideally, the Indonesian people should strongly oppose deviant behavior that harms many people by becoming a cyber crime committed by Bjorka, like previous hacking cases. However, despite the uproar that occurred at the beginning of the Bjorka case and the various concerns and criticisms of the community for him, over time the community has actually challenged and supported the hacker to open accusations of unfair acts committed by the government and its officials. Thus, this research was compiled on the basis of the question of "How did Bjorka gain popularity and public support in his cybercrime cases?"

1.2 Research purposes

This study has an objective to analyze the Bjorka case using a criminological lens to find out the factors that contributed to the success and popularity of his cyber crimes. Theoretically, this research also aims to add to the literature on cybercrime in criminology and expand the theoretical knowledge that underlies the field. As for practically, this research aims and is expected to help the understanding of policy makers and authorities in responding to, handling and preventing cybercrime in Indonesia.

II. Review of Literature

2.1 RAT (Routine Activity Theory)

Compared to focusing on the perpetrators of crime, RAT (Routine Activity Theory) focuses on the analysis of situations that give the possibility of a crime (Newburn, 2017, p. 305). Often this theory is considered a very simple theory, but the simplicity of analysis used by RAT makes this theory also flexible (Newburn, 2017, p. 304). In this case, RAT takes elements other than the motivation of the perpetrator to form a crime. In RAT, the motivation of the perpetrators of crimes is combined with two other elements, namely the appropriate target and the absence of qualified guards at the scene (Newburn, 2017, p. 305). However, it should be noted that Cohen and Felson as the originators of this theory explained (1979: 590) these three elements are elements that must be present at a minimum for a crime to take place. The presence of at least these three elements can be a factor in the success of a crime, while the loss of one of these elements can reduce the success rate of a crime.

Felson (1998: 73) once again emphasizes that apart from the perpetrators of the crime, the most important thing about the occurrence of a crime is the situation that allows the crime to occur. Besides the perpetrator and the target, a qualified guard who meant by Cohen and Felson not only to apply to police officers or other security actors, but also to apply to other individuals or groups such as families as long as the individual or group supervises the target, even if only a little. Therefore, targeting is also important in RAT. The target criteria consist of VIVA; (1) Value, (2) Inertia, (3) Visibility, and finally (4) Access (Newburn, 2017, p. 307).

For the first criterion, the actor will determine how much value the target wants to lose, the actor will choose the target if the target has a value that inspires his motivation. Then after seeing the value of the target, the perpetrator will estimate the weakness of the target, which means to consider the ease or difficulty of committing a crime that is detrimental to the target. After these two criteria, the actor seen from the RAT theory will determine how visible the target is in the sense that this target is clear to the perpetrator. In the last criterion, perpetrators will assess targets who have easier access or are more open to becoming victims of crime.

One of the most important additions to RAT is its similarity to RCT (Rational Choice Theory) in looking at the causes of crime, namely opportunity. Therefore these two theories share the same view that a criminal tends not to change his crime because he has a greater chance of success in the same field of crime (Hagan & Daigle, 2018, p. 376). Committing the same crime becomes part of the routine of a criminal where he can already predict the level of success, failure and risk of his actions compared to if the perpetrator changes direction by committing another type of crime.

III. Research Method

Qualitative methods were used to structure this research with the substance compiled using descriptive analysis. The qualitative method used is a case study and literature with secondary data. Research is structured starting with obtaining data on cybercrime in criminology, then adding cases, and analyzing them before drawing conclusions. The techniques used are data reduction and deduction techniques. The secondary data used is data and information about cyber crime and criminological theory through books and journal articles, then data about the Bjorka case and government efforts through online news portals.

IV. Result and Discussion

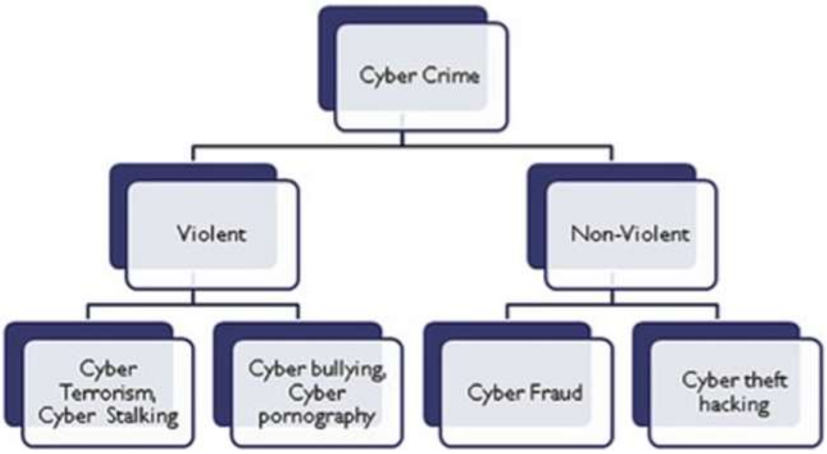
4.1 Cyber Crime in Criminology

Cybercrime is categorized as one of the fields under criminology which corresponds to one of the words, namely 'cyber' which is closely related to technology. Cybercrime is a crime that occurs in the presence of technology such as electronic devices and computers as targets (Choi et al., 2020, p. 31). In cybercrime, the types of crimes committed are mostly divided into two categories, namely crimes that utilize technology (cyber-enabled crime) and crimes that require technology to occur (cyber-dependent crime) (Dupont & Whelan, 2021, p. 79). Even though before having its own categorization in the field of cybercrime, previously cybercrime was referred to as computer crime.

This is because computer crime is more targeted at the computer device itself such as accessing a computer without permission, deliberately destroying a computer system, or stealing data on a computer (Choi et al., 2020, p. 32). Meanwhile, electronic devices are developing and are no longer just based on computer, besides that the crimes committed also no longer have a focus point only on computers. According to the United Nations (2022), cyber crime is also a form of the development of transnational crime, where this crime can cross the boundaries of place and time.

In order for a cyber crime to occur, the ecosystem within it besides the perpetrators are enablers (people who create the system to be used as a place for criminal acts), cyber guards (more towards the government or administrator of the system itself), and most importantly the existence of victims in the cybercrime ecosystem. According to Choi, et al., (2020: 33) there are several types of perpetrators of cyber crimes such as cyberpunks, terrorists who commit terrorism using cyber, newbies, computer coding experts, hackers, professional criminals, and insiders. In the various types of perpetrators, it should be noted that hackers are not entirely criminals because there are hackers who are considered as guards because they have no intention of committing crimes.

Types of crimes that are categorized as cyber crimes include many related to data, both intellectual property data, personal, company data, etc., where the data is stolen, damaged, or destroyed by cybercriminals (Thangamuthu et al., 2019 , p. 1). Meanwhile, other forms of cybercrime can be in the form of stealing money by committing fraud, extortion, etc., online. Then the destruction of someone's good name via the internet is also included in cybercrime. All kinds of online threats that use computer networks, the use of IT systems through automated processes using malware (software that functions to damage the system) and viruses, as well as various types of computer equipment are categorized as cyber crimes and have no trace. Thangamuthu, et al., (2019:


Cyber Crime
Violent
Non-Violent
Cyber Terrorism, Cyber Stalking
Cyber bullying, Cyber pornography
Cyber Fraud
Cyber theft hacking

Source: (Thangamuthu et al., 2019, p. 8)

Figure 1. *The category of cybercrime is harsh and not harsh*

This category looks at how cybercrime is offensive to individuals or groups and is detrimental, while cybercrime is not harshly non-attacking but still harms others. Through the previous explanation and the categories above, cybercrime has many forms and categorizations of attacks so that responses, policies, and ways to deal with it really require a variety of strategies. According to Pospisil, et al., (2019: 200) cybercriminals have motivations which are generally categorized into seven motivations, namely: (1) Ego,(2) Ideology, (3) Finance, (4) Revenge, (5) Challenges, (6) Feelings of Evil/Naughty, and (7) Reconnaissance. Each perpetrator will have different motivations and may have more than one motivation when committing cyber crimes.

These motivations will make perpetrators commit cyber crimes which are categorized as previously explained, namely crimes that utilize technology and requires technology such as computers and other electronic devices. In the category of crimes that require technology, according to their motivation, they are divided into types of crimes with the aim of revenge and crimes with financial goals. As for crimes that use technology, according to the perpetrator's motivation, they are divided into types of crimes with the aim of showing off, beliefs, and followers (Pospisil et al., 2019, p. 200).

4.2 Analysis of Bjorka's Cyber Crime Case

During the last two years during the Covid-19 Pandemic, the Indonesian people had to be faced with hacking cases that stole the personal data of many people. The first is a very big case in 2020, namely a data leak that occurred on Tokopedia as an online shopping site used by millions of Indonesians. Then in 2021, Indonesia will also be shocked again by the data leak experienced by the government, more precisely the Indonesian Attorney General's Office with employee data that was allegedly hacked and stolen. This theft is usually accompanied by the sale of data on several sites which are a place for hackers to sell the data they stole. In 2022, the Indonesian people were shocked again by cases of hacking and data theft that were repeated again with different actors for the third time.

A hacker using the name Bjorka first shocked the Indonesian people because he stole and sold quite important personal data belonging to the Indonesian people through Indihome data sources, KPU, and data from SIM card registration (Hardiansyah, 2022). Of course, from such a large number of sources, personal data theft exists on a fairly wide scale, from family cards, ID cards, telephone numbers, and various other confidential personal information. At first, Bjorka used the Breached forum site to sell the data he hacked. Breach myself is actually a forum site for discussion but has a special topic page where one of them is the marketplace topic which is a place for buying and selling data leaked by many hackers (Hardiansyah, 2022). At first, the sale of data carried out by Bjorka shocked the Indonesian people, but at that time the case went viral not because of Bjorka's own name, but because this was the third time a major cybercrime had hit Indonesian society. The Indonesian people at that time were still focused on cases of hacking and selling personal data themselves rather than focusing on the name of the hacker who sold their data, namely Bjorka.

However, Bjorka made his name increasingly noticed by the Indonesian people when he sold the data he hacked where the data was documents that were allegedly classified documents with the aim of receiving President Joko Widodo through data sources from the State Intelligence Agency (Nugraheny, 2022). At that time, the attention of the Indonesian people began to shift from the cyber crimes that occurred to the perpetrators of cyber crimes. In this case, the researcher looks at how Bjorka has fulfilled three elements in the RAT (Routine Activity Theory) where he has motivation as a perpetrator of crimes, although in this case if you look at the various motivations for committing cyber crimes, Bjorka could have more than one motivation other than financial motivation. Once you have motivation Bjorka has a suitable target where according to the RAT, the target is determined by VIVA—Value, Inertia, Visibility, Access (Newburn, 2017, p. 307). Where the data of the Indonesian public has access, clarity and value deemed appropriate for the data to be stolen, while the weakness (inertia) of the target (Indonesian society) is the lack of robust cyber security from the data sources it hacks.

Bjorka has the motivation and goals to match, so the third element of the RAT that he also fulfills is the absence of a qualified guard. In this context, guards are not the police or other security forces, but IT systems and programs that are less robust, as well as cybersecurity that can be hacked. In this case the researcher also see how Bjorka remained consistent in the types of crimes he committed, namely illegal hacking and selling of data, although in a more detailed context, the data he hacked was more specific towards the Indonesian government and no longer focused only on people's data. When viewed through the RAT, which focuses on analysis of the situation that led to a crime occurring, it is clear from the Bjorka case that the cybersecurity weaknesses of the government and other business entities are not robust enough to open opportunities for hackers to commit cyber crimes through these loopholes.

However, not only taking advantage of gaps in terms of cybersecurity, researchers also see how Bjorka took advantage of waves of reaction and attention from the Indonesian people who have great power to promote things. By shifting the focus of hacking to the government, Bjorka began to show himself more and more through social media such as Telegram and Twitter. Not infrequently the tweets he wrote on Twitter went viral because much of the context of his remarks was in the form of a protest against the Indonesian government wrapped in sarcasm. Many Indonesian officials appear in his various tweets, such as Puan Maharani, Johnny G Plate, Erick Thohir, Luhut Pandjaitan, and Samuel Pangerapan (Hardiansyah, 2022). When protesting covered in sarcasm, Bjorka also carried out doxing.

Support from some Indonesian people began to focus on Bjorka when he began to show himself as someone who wanted justice for society by holding protests. Although according to Dr. Ir. Ridi Ferdiana, ST, MT, IPM., as an IT expert from UGM, stated that hacktivism is a more appropriate way of placing what Bjorka was doing (Wawan, 2022). Jordan and Taylor (2004: 1) explain that hacktivism is considered as an action that is closely related to political but carried out in cyberspace by actors who are usually individuals or groups. When viewed through the wording, hacktivism is a combination of the words hack and activism which can be categorized that hacktivism is an act of hacking in order to carry out protests to social movements by utilizing technology. Hacktivism can also be seen as a place for actors to convey symbolic messages or protest against a political policy (Karagiannopoulos, 2018, p. 7).

Bjorka's hacktivism is what caught the attention of the Indonesian people, even winning the support of some Indonesians because hacktivism has appeal to people who are disillusioned with the government. This attraction was able to make the focus of the Indonesian people shift where the people should vent their disappointment and anger at Bjorka, but the subject's attention shifted to the government so that they supported cyber crimes committed by Bjorka in the form of doxing to several Indonesian government officials. Because Bjorka took advantage of suitable targets according to RAT to carry out hacktivism by looking at the visibility of the success of the actions he carried out.

4.3 Government Efforts in Handling the Bjorka Case

As discussed in the previous sub-chapter, in the RAT the government should be a capable guardian actor to prevent hacks by hackers like Bjorka. However, the absence of qualified guards made criminals have the opportunity to commit crimes which in this context are cybercrimes in the form of hacking, especially at the start of Bjorka's presence, who sold Indonesian people's personal data through sources such as KPU and SIM Card registration. Indonesia itself already has a BSSN (National Cyber and Crypto Agency) as an agency that already has clear objectives to work in the field of cyber security (BSSN, 2022).

Even though the BSSN is classified as an agency that was only formed about five years ago in 2017, it is a fusion of several other state agencies such as the State Crypto Agency, then the Directorate of Information Security, the Directorate General of Informatics Applications, and the Ministry of Communication and Information—You could say that even though as an agency BSSN is relatively new, but BSSN's experience in cybersecurity is not new. In carrying out its duties, the BSSN has eight functions (BSSN, 2022):

1. Formulation and establishment of technical policies in the field of cyber security and passwords
2. Implementation of technical policies in the field of cybersecurity and passwords
3. Compilation of norms, standards, procedures and criteria in the field of coding
4. Implementation of technical guidance and supervision in the field of coding
5. Coordination of task implementation, coaching, and administrative support to all organizational elements within the BSSN
6. Management of state property which is the responsibility of BSSN
7. Implementation of substantive support to all elements of the organization within the BSSN
8. Supervision of the implementation of tasks within the BSSN

These eight functions are carried out to carry out the main task of the BSSN, namely to assist the President in running the government by taking part in government tasks in the field of cyber security and national cipher (BSSN, 2022). One of the eight functions of the BSSN, namely the number one and two functions related to the formulation and determination of policies, then the implementation of the policy is technically closely related to the role of the BSSN as an institution that provides cyber security at the national level. However, BSSN is still unable to become a guardian that provides solid cyber security for Indonesia so it does not extinguish elements the third is from the RAT when the BSSN has the function to carry out technical policies in carrying out cyber security.

Ideally, the presence of BSSN should be more than sufficient to respond to cyber crimes committed by Bjorka, but the Indonesian government realizes that for this case not only must the government capture the identity and whereabouts of Bjorka, but also must quickly improve, fix and managing cyber security at the national level so that the public can return to giving their focus and trust to the government. Thus, when the Bjorka case occurred, President Joko Widodo formed an emergency response team which was a combination of BSSN, BIN, Kominfo, and Cybercrime Bareskrim Polri (CNN Indonesia, 2022), where the team is said to have a duty to restore the faith in the government that was ripped from the people by Bjorka's hacking and hacktivism. Because in this case situation, the government is trying to restore people's trust in the government's responsibility for their security through actions that produce real results.

V. Conclusion

Indonesia is a country that is no stranger to cases of hacking and data theft by various hackers. However, the intensity of Indonesian data theft has increased during the Covid-19 pandemic, where many people are getting closer to technology because of the demands of the situation that requires everyone to do all activities from home for the last two years. A very interesting case among the last three years is the case in 2022 which is the case of the theft and sale of data by a hacker by the name of Bjorka. The attractiveness of this case lies in the phenomenon where people's attention shifts from the main concern, namely cyber crime cases turned to disappointment with the government which was manifested in the form of support for Bjorka as the perpetrator of cyber crimes.

Looking at the Bjorka case based on the RAT (Routine Activity Theory) in criminology which contains: (1) The motivation of the perpetrators, (2) Appropriate targets, (3) The absence of qualified guards—In short, it can be seen that Bjorka's most important motivation is financial motivation because the cyber crime that was published to the public for the first time was the sale of people's personal data. However, as Bjorka's cyber crime progresses, his motivation as a perpetrator also increases. Bjorka is increasingly showing that he is targeting the Indonesian government by allegedly leaking secret Presidential data to doxing several government officials which leads to other possible motivations such as challenge and ego.

What distinguishes Bjorka's case from hacking cases in 2020 such as Tokopedia and 2021 such as the hacking of the Indonesian Attorney General's Office is how the objective of cybercrime cases does not only focus on the business of illegally buying and selling data, but leads to criticism and protests against the government which get attention, curiosity , as well as empathy from the majority of Indonesian people. Bjorka's name has soared high along with his cyber crime case which has become increasingly viral among the public. Attention that is actually focused on the government's mistakes compared to actual cyber crimes is considered to be misguided. This is caused by Bjorka's method of using hacktivism in which he combines a crime, namely hacking with activism.

References

BSSN. (2022). Tentang BSSN. BSSN.go.id. Retrieved October 26, 2022, from https://bssn.go.id/tentang-bssn/

Cambridge Dictionary. (2022, October 19). DOXING | English meaning - Cambridge Dictionary. Cambridge Dictionary. Retrieved October 26, 2022, from https://dictionary.cambridge.org/dictionary/english/doxing

Choi, K.-S., Lee, C. S., & Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer International Publishing.

CNN Indonesia. (2021, February 17). Database Kejaksaan RI Diretas, Hacker Sebut Jokowi dan UU ITE. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20210217152812-185- 607441/database-kejaksaan-ri-diretas-hacker-sebut-jokowi-dan-uu-ite

CNN Indonesia. (2022, September 12). Jokowi Bentuk Tim Khusus Respons Serangan Bjorka. CNN Indonesia. https://www.cnnindonesia.com/nasional/20220912162500-32-846753/jokowi- bentuk-tim-khusus-respons-serangan-bjorka

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Dewi, I. R. (2022, September 14). Bikin Heboh RI, Data Apa Saja yang Dibocorkan Hacker Bjorka? CNBC Indonesia.https://www.cnbcindonesia.com/tech/20220914095826-37-371939/bikin-heboh-ri-data-apa-saja-yang-dibocorkan-hacker-bjorka?page=all

Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. Journal of Criminology, 54(1), 76–92.10.1177/00048658211003925

Fedotov, Y. (2017, October 23). In Just Two Decades, Technology Has Become A Cornerstone Of Criminality. unodc. Retrieved October 26, 2022, from https://www.unodc.org/unodc/en/frontpage/2017/October/in-just-two- decades--technology-has-become-a-cornerstone-of-criminality.html

Felson, M. (1998). Opportunity Makes the Thief Practical theory for crime prevention. Police Research Series Paper, 98.

Franedya, R. (2020, May 7). 91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta- data-pengguna-bocor-tokopedia-digugat-rp-100-m

Hagan, F. E., & Daigle, L. E. (2018). Introduction to Criminology: Theories, Methods, and Criminal Behavior. SAGE Publications.

Hardiansyah, Z. (2022, September 7). Apa Itu Breached Forums yang Terlibat 4 Kasus Kebocoran Data di Indonesia Sebulan Terakhir? Halaman all - Kompas.com. Kompas Tekno.https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached- forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia?page=all

Hardiansyah, Z. (2022, September 12). Rentetan Aksi Hacker Bjorka dalam Kasus Kebocoran Data di Indonesia Sebulan Terakhir Halaman all - Kompas.com. Kompas Tekno. Retrieved October 26, 2022, from https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker- bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan

Jordan, T., & Taylor, P. (2004). Hacktivism and Cyberwars: Rebels with a Cause?Taylor & Francis.Karagiannopoulos, V. (2018). Living With Hacktivism: From Conflict to Symbiosis(V. Karagiannopoulos, Ed.). Springer International Publishing.

Newburn, T. (2017). Criminology. Routledge.

Nugraheny, D. E. (2022, September 10). Ini Dokumen yang Diklaim Milik Jokowi dan Diunggah Hacker Bjorka, Ada yang Diberi Label Rahasia. Kompas.com. https://nasional.kompas.com/read/2022/09/10/15331111/ini-dokumen-yang- diklaim-milik-jokowi-dan-diunggah-hacker-bjorka-ada-yang

Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. Journal of Ethics and Legal Technologies (JELT), 2(1), 48-74.

Pospisil, B., Huber, E., Quirchmayr, G., & Seboeck, W. (2019). Modus Operandi in Cybercrime. In M. Khosrowpour (Ed.), Encyclopedia of Criminal Activities and the Deep Web, VOL 1. IGI Global.

Song, D. (2018). What Is Cybercrime? A Criminology Perspective. Journal of the MTA-DE Public Service Research Group, 3(2), 11-15. DOI 10.21868/PGnG.2018.2.2.

Thangamuthu, P., Rathee, A., Palanimuthu, S., & Balusamy, B. (2019). Cybercrime. In M. Khosrowpour (Ed.), Encyclopedia of Criminal Activities and the Deep Web, VOL 1. IGI Global.

UNODC. (2022). Cybercrime. United Nations Office on Drugs and Crime.Retrieved October 26, 2022, from https://www.unodc.org/unodc/en/cybercrime/index.html

Wawan, J. H. (2022, September 13). Soal Bjorka, Begini Tanggapan Pakar IT UGM tentang Kebocoran Data. Detikcom. https://www.detik.com/jateng/jogja/d-6289696/soal-bjorka-begini-tanggapan-pakar-it-ugm-tentang-kebocoran-data?utm_source=copy_url&utm_campaign=detikcomsocmed&utm_medium=btn&utm_content=jateng%20Baca%20artikel%20detikjateng,%20%22Soal%20Bjorka,%20Begini%20T