Cyber Security Analysis and Law; Bjorka Case

Aldiyan Harun Prasetyo, Emmy Latifah
Department of International Relations, Faculty of Social and Political Science, Sebelas Maret University
Surakarta, Indonesia
aldiyanhp14@student.uns.ac.id

Article Information

Submitted :
Accepted :

Keywords :
Technology; Cybersecurity; Indonesia; Government

Abstract

Technology has always been a powerful tool for advancing human civilization. It had allowed us more organized, efficient, and connected. Since the dawn of the Internet, we have increasingly relied on electronic communications as a means of doing business. Cybersecurity, which also encompasses authentication, non-repudiation (non-denial), and accountability, is an effort to safeguard the confidentiality, integrity, and accessibility of information in cyberspace. The process of defending computers, servers, mobile devices, electronic systems, networks, and data from hostile attacks falls under the category of cybersecurity. The following questions are used to evaluate the descriptive data in this paper, which employs a qualitative management approach: What prompted hackers to inflitrate Indonesia and How is the government responding.

INTRODUCTION

Technology has always been a powerful tool for advancing human civilization. It had allowed us more organized, efficient, and connected. However, as technology becomes more and more advanced, there is a greater risk of its misuse. This is a particular problem when it comes to electronic communication.

Since the dawn of the Internet, we have increasingly relied on electronic communications as a means of doing business. Unfortunately, this makes the Internet a breeding ground for hackers and criminals looking to exploit weak security settings. The convenience of conducting daily business online carries with it a significant risk of personal and confidential information being stolen by malicious actors. This can be very harmful, especially for businesses. Loss of sensitive company data can irreparably damage the reputation and jeopardize financial stability.

To solve this problem, technology companies are investing heavily in the development of new security measures and procedures to prevent unauthorized access. As new threats emerge, they are quickly addressed through the use of advanced encryption methods and sophisticated computer algorithms. While these preventative measures have made internet use much safer than it used to be, they are still not foolproof and there are often gaps in their defenses.

Technology is vital to making organizations and people the computer safety tools required to protect themselves from cyber-attacks. Three primary entities must be protected: Endpoint devices like calculators, intelligent devices, and routers; webs; and this cloud. General technology used to defend these entities include next-generation firewalls, DNS filtering, malware security, antivirus code, and e-mail protection solutions.

However, Indonesia was conceded by hackers. On a dark web forum, a user by the name of Bjorka claims to have hacked the security system of the Indonesian government and taken the information therein. The information collected includes the user's name, email address, NIK, NPWP, phone number, and expenditures. Additionally, a link is provided that shows instances of account information and transactions made using the data.

Additionally, Bjorka has accounts on Twitter and Telegram. Bjorka frequently

appears to be disseminating the information he has acquired there. And frequently seen to tweets about how poorly the Indonesian government controls the security system.

Previously, the Indonesian people were astonished by what Bjorka was doing and what kind of purpose by doing that. And surprisingly, Bjorka shared his motives for what he has been doing, especially making tweets on Twitter like a 'bait'.

In Warsaw, Poland, where he was discovered to be from the same location, Bjorka said that he had a good buddy from Indonesia there. Moreover, Bjorka advised the Indonesian government against attempting to find his closest friend's whereabouts because doing so would be pointless using the foreign ministry. Despite the fact that his best friend was intelligent, the reason was that due to the 1965 policy, he was no longer an Indonesian citizen.

Bjorka further claimed that he carried out his dear friend's intentions by doing so. According to reports, his pal still has unrealized ambitions to really go back to Indonesia, where he was born, and "do something with tech even though he realizes how miserable it is to be a Habibie."

Bjorka recognizes that it is hard to carry on his best friend's ambition, who has supposed to take care of him since childhood, in the same way. As a result, Bjorka decides to find a different solution so that his best friend's home country can improve.

METHODOLOGY

A. Literature Review

Agus Subagyo in his journal article entitled Synergy in Facing Cyber Warfare Threats said that in the era of globalization, the nature of threats does not only come from military and physical aspects alone, but also comes from non-military and non-physical threats, one of which is cyber threats. The world has now entered the cyberspace era which gave rise to cybercrime and has the potential to pose a threat of cyberwar. Indonesia needs a cyber army to fight the threat of cyber war. The Ministry of Defense of the Republic of Indonesia must be at the forefront of the process of developing cyber defense policies to counter the threat of cyber warfare. Synergy between stakeholders and related parties in the fight against cyber warfare is the key to success.

In this regard, changes are constantly taking place in a dynamic world, sometimes colored by disturbances that affect relations between countries and the totality of global problems that affect the foundations of national and state life. Every global event in the world will always affect the entire life of the country in every country, forcing every country to always observe and analyze every event in a strategic environment both at the global, regional, national and local levels.

Paulina Pannen in her article in the journal Quality Assurance in Online Learning and Scale at Indonesia Cyber they-go-free journal in the journal journal Journal Journal article at Indonesia Cyber Education Institute, The adoption and implementation of online education aims to improve the quality of teaching and learning, taking into account others' different student learning styles, increasing access to learning opportunities, increasing learning flexibility for students to develop the necessary skills and abilities and improving the cost effectiveness of the institution . Online education allows everyone to study anytime, anywhere; as well as communicating and collaborating virtually from different countries. The introduction and implementation of online education aims to improve the quality of teaching and learning, taking into account the different learning styles of students, increasing access to learning opportunities, increasing flexibility in education for students to develop the skills and abilities needed in the twenty-first century, and increasing the cost-effectiveness of institutions.

B. Data gathering Method

The following questions are used to evaluate the descriptive data in this paper, which employs a qualitative management approach: What prompted hackers to inflitrate Indonesia and How is the government responding.

ANALYSIS

A. The Category of Cyber Security and the Part of it

Cybersecurity, which also encompasses authentication, non-repudiation (non-denial), and accountability, is an effort to safeguard the confidentiality, integrity, and accessibility of information in cyberspace. The process of defending computers, servers, mobile devices, electronic systems, networks, and data from hostile attacks falls under the category of cybersecurity. It is often referred to as electronic information security or information technology security. The phrase can be broken down into a number of broad categories and is used in a wide range of contexts, including business and mobile computing.

There are six categories which in Cybersecurity, inter alia, 1. Network security is the process of protecting communications systems from intruders, such as deliberate attackers or malicious software that strikes at random; 2. Application security aims to protect devices and software against threats. Applications that have been compromised may give users the access to the information they were meant to guard. Long before software or machines, layout is where successful security begins; 3. Data protection, integrity of records and privacy are safeguarded by data protection both at certain points of storage and transmission; 4. Operational safeguards consist of procedures and choices made to manage and protect information properties. This includes protocols that describe where and how data can be stored or transferred as well as customers' rights when gaining access to community; 5. Disaster recovery and business continuity is to how a company responds to cyberattacks or other events that cause a loss of operations or data is defined by business continuity and disaster recovery. The organization's procedures for restoring activities and information to their pre-incident state are outlined in the disaster recovery policy. When an organization tries to function without specific resources, its plans fall back, which is known as business continuity; 6. It offers end-user training with the human element of cybersecurity, which is patchy at best. anyone who ignores a good security strategy has the ability to accidentally introduce a deadly disease into a secure system. The security of any company depends on its employees learning how to remove suspicious email attachments, avoid connecting unknown USB devices and many other important lessons.

B. The Indonesian Governments' Strategy Against the "Hacking"

The national strategy of Indonesia consists of six main areas, inter alia 1. culture and capability of information security; 2. Risk of Information security; 3. risk reduction in terms of information security; 4. events involving information security; 5. Performance in information security management; 6. capabilities for law enforcement in the area of ITE.

The vision and mission of the ministry of communication and informatics' cyber security plan are also stated there. Its vision is to assure the execution of digital transformation within the context of electronic-based government, the digital economy, and knowledge-based citizens, its objective is to create a safe, dependable, and responsible information ecosystem. While its mission is to construct and manage cyberspace in a way that is dependable, responsible, and safe while also defending the interests of the country of Indonesia.

There are cybersecurity goals, within; Cyber Resilience, the establishment of a national critical data infrastructure, which under this strategy must be robust to attacks and capable of continuing to provide services to the general public even if it is damaged or destroyed partially; Cyber public service, the development of strategies, actions, and procedures for dealing with and recovering from insider threats and cyberattacks through information exchange, teamwork, and action tactics; Cyber law enforcement, the creation of a framework as well as the application of regulations and laws that can produce a secure and friendly online environment; Cybersecurity

culture, In this case, culture refers to a standard evaluation and way of thinking while tackling information security challenges. fostering a culture of cybersecurity that encourages safety and responsible Internet use; Cyber secure market, The formation of capacity, competence, and cyber security.

Leaving that apart, there are two distinct categories of cyberattackers: crackers and hackers. In the realm of computer hacking, the term "hacker" is well-known; nevertheless, another phrase, "cracker," is also widely used. Despite having similarities at first glance, the two are not identical in terms as to how they operate or their objectives. if the hacker uses malware to commit crimes. Meanwhile, hackers do not hack for illegal reasons.

Hackers assist businesses or other worthwhile causes by using their knowledge of operating systems and programming. Hackers strive to safeguard data and strengthen corporate security. Hackers uncover security gaps in businesses and close them to make them tighter or safer. Data theft, network harm, and system harm are not goals of hackers.

C. Some Different Types Between the Hackers Based on their "Hat"

Hackers come in a variety of types, including black hat, white hat, and gray hat. Black hat hackers are internet criminals who deliberately breach networks without permission. Black hat hacking is defined as an attempt to gain unauthorized entry to a target computer system. Once black hat hackers discover a security flaw, they try to exploit it, usually by introducing malware such as trojans or viruses.

Black hat hackers often start out as inexperienced "script kids", using commercial hacking tools to exploit security vulnerabilities. Some are taught to hack by employers looking to make some quick money. The most well-known black hats are usually expert hackers working for highly organized criminal groups that occasionally offer their employees communication tools and customer service agreements, such as a common business. Sometimes, black hat malware kits sold on the dark web come with warranties and customer support.

Black hat hackers frequently specialize in particular areas, including administering remote access tools or phishing. From forums and other links on the dark web, many people find their "work." Others, like in the normal business world, choose to work via franchises or leasing agreements, but some choose to create and sell malicious programs directly. Governments now use hacking as a crucial weapon for acquiring intelligence, although the black hat typically work either alone or with organized crime groups in exchange for quick cash.

Due to its size, hacking can function like a huge company, making it simple to stretched harmful software program. Organizations have companions, resellers, vendors, and affiliates, and that they buy and promote malware licenses to different criminal enterprises for utilization in new markets or locations.

Some black hat businesses also have contact facilities that they use to make outbound calls while posing as employees of well-known software companies like Microsoft. Hackers in these scams try to persuade potential victims to download software or provide full access to their systems. By allowing access to or installing the proposed software, victims unwittingly give criminals the ability to collect passwords and banking information, secretly take over computers, and use them to - attack others. To worsen the damage, victims are often judged to be outrageously expensive for this "favor". Other hacks involve no human interaction and are quick and automated. Attack bots search the internet in these situations for devices that can be easily hacked, usually through phishing, virus attachments, or connections to hacked websites.

Black hat hacking is a widespread issue, making it very challenging to eradicate. Hackers frequently leave little evidence, exploit the computers of unknowing victims, and cross various jurisdictions, which presents difficulties for law enforcement. Authorities may occasionally be successful in closing down a hacking portal in one nation, but the same

operations may continue in another, allowing the organization to continue.

Consequently, White hat hackers are ethical security intruders who locate and patch holes. White hat hackers try to discover system flaws so they may be fixing and assisting to increase a device's basic safety. They hack into databases with the consent of the agencies they hack into. White hat hackers utilize their abilities to locate security flaws to assist in protecting enterprises from harmful hackers. They may occasionally be salaried staff or independent contractors who search for security flaws on behalf of businesses.

Larger firms often experience fewer website issues and halt due to white hat hackers. Most hackers realize that accessing systems operated by large corporations will be more difficult than systems operated by smaller businesses, which likely do not have the capacity to thoroughly analyze security vulnerabilities. Penetration testers, on occasion called "pentesters", are a subclass of ethical hackers who focus specifically on identifying vulnerabilities and evaluating risks in systems.

White hat hackers appoint the identical hacking strategies as black hats. But, the crucial distinction is they attain the gadget proprietor's consent first, making the technique completely felony. White hat hackers collaborate with network admin to quick remedy issues before they may be noticed with the aid of other customers, rather than the usage of vulnerabilities to propagate programs.

White hat hacker skills and tactics includes; 1. Social engineering, occasionally called "people hacking," is a frequent tactic utilized by white hat hackers to become aware of gaps in an agency's "people" defenses. The purpose of social engineering is to manipulate and mislead sufferers into acting inappropriately (making wire transfers, sharing login credentials, and so forth); 2. Penetration testing, Penetration testing aims to identify vulnerabilities and vulnerabilities of endpoints and defenses so they can be fixed; 3. Reconnoiter and research, this entails investigating the company to find weaknesses in the IT and physical infrastructure. The goal is to gather enough knowledge to find legal ways to bypass security measures and controls without causing damage or harming anything.; 4. Programming, White hat hackers create honeypots that act as gimmicks to lure criminals online, distract them, or help white hats learn valuable details about attackers.; 5. Utilizing a variety of analog and digital techniques, This comprises the tools and equipment that enable the vulnerability testers to access the servers or network and install malware such as bots.

The procedure is made more enjoyable for certain white hat hackers through the use of bug bounty schemes, which are contests that offer financial rewards to participants who identify security flaws. Even training programs, conferences, and certifications are available for ethical hacking.

The different between Black hat and White hat is motivation. White hat hackers collaborate with corporations to discover systemic flaws and connect them, in contrast to black hat hackers who illegally gain admission to systems with adversarial motives and regularly for private gain. They do this to prevent unauthorized entry to the system's information via black hat hackers.

Moreover, there are Grey hat hackers. Even as grey hat hackers may not have the identical illegal or malevolent purpose as black hat hackers, they nonetheless lack the expertise or permission of the organizations whose systems they're breaking into. However, gray hat hackers are not absolutely exploit gaps they discover, which include zero-day flaws; instead, they document them. But, Gray hat hackers can request charge in return for full disclosure of what they determined.

Gray hat hackers sometimes want to assume that by way of breaking into organizations' networks and web sites with out authorization, they are reaping rewards the ones companies. However, business owners rarely receive intrusions into their information infrastructure. The real motivation of gray hats is to demonstrate their capabilities and gain recognition for what they see as cybersecurity services.

While grey hat hackers once in a while spoil the law or well-known ethical standards, they lack the malicious reason more than a black hat hacker. If a white hat hacker reveals a weak point, they will handiest use it with consent and maintain it a secret till it's been constant. The black hat, however, will take benefit of it illegally or educate others on the way to do it. the grey hat won't coach others on the way to illegally abuse it both.

It's the goal of many gray hats to make the internet safer for people and businesses because they don't think it's safe for commerce. To prove their point and spread havoc, they accomplish this through hacking networks and websites. Gray hats frequently claim that their incursions are harmless. Sometimes they just want to hack a famous system out of curiosity, disregarding privacy rules and several other restrictions.

Most of the time, gray hats offer businesses useful information. However, the white hat community and a large portion of the online community do not consider their strategies to be moral. Gray hat hacking is prohibited because no organization allows hackers to try to break into their network.

Grey hat hackers may recommend to the system authority that they or one among their friends be paid to remedy the problem after successfully gaining unauthorized entry to a network or device. But, due to corporations' growing readiness to sue, this tendency has been on the decline.

Some agencies rent worm bounty schemes to lure black hat hackers to publish their discoveries. In these conditions, companies provide a praise to lessen the risk that the hacker may additionally use the vulnerability for non-public advantage. But, as that is not often the case, the handiest way to make sure that a hacker is in compliance with the regulation is to attain the company's authorization. And maybe, gray hat hackers could occasionally turn into black hats by publishing the point of exploit online or even using the vulnerability themselves if corporations do not act quickly or comply.

The big gap different between grey hat and white hat is that the gray hat hacker is not constrained by ethical hacking standards or an employment contract if a business chooses to ignore him or her. Instead, they could decide to use the vulnerability themselves or spread the information online for use by other hackers.

And lastly but not a most, there is a cracker employee. Operating systems and programming are further areas of expertise for Cracker. Crackers, however, use hacking for illegal activities. Typically, crackers target the computer systems of other businesses or people in order to gain profit and hurt their victims.

Crackers operate by scanning a network for security flaws before erasing and capturing the data. Hackers have the ability to compromise systems and misuse data. Crackers typically use devices and IP addresses that are hard to track.

D. Which Side Bjorka Prefers, and Indonesian Government Reactions to 'his' Action

As said in the first chapter, Bjorka wants to grant the request of her Indonesian best friend. Unfortunately, the 1965 policy prevented Bjorka's best friend from granting his own desire. By sharing information and data he has gotten from the Indonesian government and businesses, Bjorka hopes to help his friend realize his ambition. Bjorka also alerts the government to the fact that Indonesia's cyber security system is quite shoddy.

Bjorka impersonates a Black Hat Hacker and unintentionally switches to a Gray Hat Hacker as well. Bjorka makes an account on Twitter and Telegram and frequently appears to be disseminating the information he has acquired there and had seen to tweets about how poorly the Indonesian government controls the security system.

Regardless of his allegiance, Bjorka has illegally gained access to the security systems of both the Indonesian government and private businesses. Bjorka also alleges that she sold information obtained from a dark forum. Clearly, the Indonesian government addressed this issue directly. The Indonesian server's

account for Bjorka was promptly deleted, and more action was taken by the authorities.

The government responded to Bjorka's existence by passing Law of the Republic of Indonesia Number 27 of 2022 Concerning the Protection of Personal Data. According to Article 3 this law is founded on security, regulatory quality, legitimate interests, efficiency, prudence, balance, accountability, and confidentiality.

Sri Mulyani Indrawati, the Republic of Indonesia's Minister of Finance, underlined the significance of cyber security in the current all-digital era. The reason is that government websites have frequently been the target of hacker or hacker attacks. despite the risk of sensitive government information being stolen. Other nations, besides just Indonesia, are also quite susceptible to hacking, which can obviously hurt a lot of people or parties.

Herein lies the value of cyber security. Cybersecurity is the practice of defending systems, networks, software, and data from online dangers and unauthorized access, notably from hackers. Cyberthreats not only target big enterprises; they also target small businesses and people. For instance, accessing private information, altering crucial data, or even erasing it.

Article 31 of Law of the Republic of Indonesia Number 19 of 2016 Concercing Information and Electronic Transactions, explain (1) Everyone intentionally intercepts or wiretaps other people's electronic information and/or electronic documents in a computer or other electronic system without their consent or in violation of the law; and (2) Anyone who unlawfully intercepts the transfer of information of electronic information or documents that are not in the public domain from, to, or inside a specific computer or electronic system owned by another person, whether they do so intentionally and without authorization or whether they do so by changing, omitting, or terminating the transmission of electronic information or documents.

Article 40 of Law of the Republic of Indonesia Number 19 of 2016 Concercing Information and Electronic Transactions, explain (2) In accordance with the requirements of laws and regulations, the government safeguards the public interest against all types of disruptions caused by the misuse of digital data and transactions that upset public order. continued (2a) In accordance with the terms of applicable laws and regulations, the government is required to stop the transmission and use of digital data and/or documents that include banned content. then (2b) In order to carry out the prevention mentioned in paragraph (2a), the Government has the power to restrict access to electronic information and/or documents that include illegal material, and/or to require the electronic system operator to do so.

CONCLUSION

Technology has always been a powerful tool for advancing human civilization. It had allowed us more organized, efficient, and connected. Since the dawn of the Internet, we have increasingly relied on electronic communications as a means of doing business. Unfortunately, this makes the Internet a breeding ground for hackers and criminals looking to exploit weak security settings. To solve this problem, technology companies are investing heavily in the development of new security measures and procedures to prevent unauthorized access. As new threats emerge, they are quickly addressed through the use of advanced encryption methods and sophisticated computer algorithms. However, Indonesia was conceded by hackers. Even if you believe that your personal information and data is secure, we are unable to ignore this reality. Despite the fact that we have been given authority, we are not always exempt from accountability. The data gained may be misused by hackers and crackers for their own or collective goals. It may be for sale, use a false identity, or serve other purposes. The main thing is that we are each responsible for, interested in, and owning our own personal information. Don't even give a random people access to your sensitive information, even they are your close friend.

Don't tell someone who demands personal information under the guise of being from the government. If you receive a link from an unknown number or email, don't click on it because the hacker can then track your personal information.

BIBLIOGRAPHY

[1]"UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi [JDIH BPK RI]," *peraturan.bpk.go.id*. https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022 (accessed Dec. 29, 2022).

[2]C. N. N. Indonesia, "Siapa Bjorka dan Kenapa 'Mengacak-acak' Indonesia?," *teknologi*, Oct. 12, 2022. https://www.cnnindonesia.com/teknologi/20220912053812-192-846395/siapa-bjorka-dan-kenapa-mengacak-acak-indonesia (accessed Dec. 29, 2022).

[3]Kaspersky, "What is Cyber Security?," *Kaspersky.com*, 2019. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (accessed Dec. 29, 2022).

[4]R. K. Siregar, "Perbedaan Hacker dan Cracker," *www.djkn.kemenkeu.go.id*, Sep. 27, 2022. https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/15422/Perbedaan-Hacker-dan-Cracker.html (accessed Dec. 29, 2022).

[5]Kaspersky, "Black hat, White hat, and Gray hat hackers – Definition and Explanation," *www.kaspersky.com*, Apr. 09, 2021. https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (accessed Dec. 29, 2022).

[6]O. Buxton, "Hacker Types: Black Hat, White Hat, and Gray Hat Hackers," *Hacker Types: Black Hat, White Hat, and Gray Hat Hackers*, Oct. 12, 2022. https://www.avast.com/c-hacker-types#:~:text=White%20hat%20hackers%20probe%20cybersecurity (accessed Dec. 29, 2022).

[7]"UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik [JDIH BPK RI]," *peraturan.bpk.go.id*. https://peraturan.bpk.go.id/Home/Details/37582/uu-no-19-tahun-2016 (accessed Dec. 28, 2022).

[8]A. Chendramata, "Indonesia Cyber Security Strategy," *dephub.go.id*. https://dephub.go.id/public/files/uploads/posts/posts/postbody/strategi_cs_nasional_desember2016.pdf (accessed Dec. 28, 2022).

[9]I. R. Dewi, "Hacker Bjorka is Back, Data Apa Saja yang Pernah Dibocorkan?," *CNBC Indonesia*, Nov. 11, 2022. https://www.cnbcindonesia.com/tech/20221111075351-37-386931/hacker-bjorka-is-back-data-apa-saja-yang-pernah-dibocorkan (accessed Dec. 28, 2022).

[10]

A. Subagyo, "SINERGI DALAM MENGHADAPI ANCAMAN CYBER WARFARE," *Jurnal Pertahanan & Bela Negara*, vol. 5, no. 1, Aug. 2018, doi: https://doi.org/10.33172/jpbh.v5i1.350.

[11]

P. Pannen, "Quality Assurance in Online Learning at Scale at the Indonesia Cyber Education Institute," *Education in the Asia-Pacific Region: Issues, Concerns and Prospects*, pp. 121–134, 2021, doi: https://doi.org/10.1007/978-981-16-0983-1_9.