Analytical Study of Indonesian Cybersecurity: Lesson Learned From Estonian Cyberattacks In 2007

Adiningtyas Dwiputri Samsoerizal[1], Eri Radityawara Hidayat[2], Achmed Sukendro[3]

[1,2,3]*Peace and Conflict Resolution Department, Indonesia Defense University, Indonesia*

ABSTRACT: The development of technology caused the possibility of non-conventional war that can't be predicted by human's intelligence. Cyber becomes the most vulnerable media for war. Because this media offers the attacker to hide its identity and attack anyone they want. In some case cyber-attack could cause stoppage of a country's activity if cyber is one of the country's most important thing. The cyber-war of Estonia in 2007 was the first and biggest cyber-war towards a country in history. The attack could cause the stoppage of the country's activity. Russia was the only possible one to blame. In order to react to this case Estonia called NATO for help to finish the case.As the world went to 4.0 industrial revolution era, Indonesia needed to also be aware of cyber attacks. Therefore, Estonian Cyberattacks should become reflection and awareness for Indonesia in deterring possible cyberattacks in the future.

Keywords: Cyber-war, Estonia, Russia, NATO, Indonesia

I. INTRODUCTION

Estonia is a well-developed country that has a major development in technology and information. This could be proven by the abillity of Estonia in 1998 to facillite internet access for every computer in the country. The dependency of Estonians to internet supported by the Government through the human rights policy for every Estonians to get access for internet in 2000(Psaila, 2011). This made Estonia to become the country with the best internet facility in Europe and the world. The relationship between Estonia and internet network had enact the Government to utilize the internet access for the better living of Estonians by creating software program named, X-Road, as the central database for every Estonians since they were bornto their death(X-Road, 2019).But this huge development of technology and information had come to the doom, when Estonians were shocked by the down on internet access all around the country.At that time, all aspects of the lives of Estonians and the Government that depended on the internet were suddenly disconnected. Which makes all the activities of the state paralyzed. It is known, the incident was the work of Russian hackers who deliberately carried out cyber attacks in a country that relies heavily on internet access. The cyberattack was the first and largest cyberattack against a country in history(The Economist, 2010).

Indonesia as one of the developing country in the 4.0 industrial revolution era, needs to be more aware of this alarming event. As internet is now part of every life in the country, even the smallest activities such as entertainment to the major activities such as work and Governmental activity should be accessed through internet. And not to mention, the pandemic of Covid-19 in 2020 also played major role in the major dependency of internet. Therefore, Indonesia should maintain a more developed and greater cybersecurity system to deter more possible attacks coming from the internet platform. This is inseparable from the fact that Cyber warfare has become one of the most worried warfare during the era(Fry, 2010).The Covid-19 pandemic, in addition to triggering a significant increase in phishing attacks, spams and ransomware attacks, has also increased the pressure to establish a well-functioning cybersecurity infrastructure(CIPS Indonesia, 2021).

II. Methods

Research method used by researchers this research is qualitative with data collection techniques literature reviews from journals, articles, and books related to the issue. This is the most common techniques used in qualitative research that is proposed by John W. Creswell. The research objects in this study are the Cyberattacks of Estonia in 2007 and the lesson learned for Indonesia by reflecting the cyberwar between Estonia and Russia in 2007.

III. Result and Discussion

Cyber Attacks on Estonia

Cyber-attacks is a type of attacks with offensive nature that target computer information systems, infrastructure, computer networks, or personal computer devices. Referring to the type and activity of the attack, cyberattacks can be categorized as cyber campaign, cyberwarfare and cyberterrorism. Cyber attacks can be carried out by nation-states, individuals, groups, communities or organizations. Cyber attacks may come from anonymous sources. Cyberattackers can steal, alter, or destroy specific targets by hacking into vulnerable systems. In some cases the perpetrators of cyber attacks can attack the entire government system of a country(Lin & Tom, 2016).

Cyber-attacks occurred in a country in Northern Europe, namely Estonia, on April 27, 2007. This attack was carried out by hackers with the alleged motive behind this attack being a protest against the demolition of a monument to Russian soldiers in the city of Tallinn, the capital of Estonia. These cyber-attacks targeted the websites of Estonian organizations including the Estonian parliament, banks, ministries, newspapers and broadcasters. This attack resulted in paralysis of government operations, the economy, banking, online news channels, public services and citizen activities. According to Aviksoo, the Estonian Minister of Defense, the attack was part of a global political agenda aimed at weakening the credibility of the Estonian government(McGuinness, 2017).

Timeline of Estonian Cyber Attack

For three weeks from 27 April to 18 May 2007, components of Estonia's Internet infrastructure were subjected to Distributed Denial of Service (DDoS) attacks, websites, DNS server attacks, mass e-mail, and spam comments. This cyberattack was first discovered after the Estonian government's policy to remove statues of soldiers in Tallinn. At that time, the Russians in Estonia felt that the statue marking their struggle during the Second World War was not considered special by the Estonian Government and caused protests in the local Russo-Estonian community. Shortly after that on 27 April 2007, Estonians first became aware of a cyber attack through inaccessible banking activities. It turned out that the same thing happened not only in banking activities but in every important access of Estonia such as parliamentary sites, government, economy, online news channels, public services to citizen activities(Schmidt, 2013).On April 30, after a massive attack on the country's vital networks there was also an attempt by hackers to stop the entire public sector communications network. On May 1 and 2 there were three larger scale attacks, but after that the volume of attacks stabilized. On May 3 there was an attack on government websites and government agencies, the attack used was a large-scale DDoS, and was accompanied by attacks on Estonian media outlets and websites of private companies. There has also been an increase in the number of spam emails(Zahra, 2021).

On May 5 and 6, attacks continued in a relatively similar fashion but on a smaller scale and on May 8 a larger and longer attack on government websites and communications networks was carried out. According to sources, the attacks targeting government institutions used a scale almost 400 times larger than the normal scale and this attack originated outside Estonia. It is known that some Russian hackers managed to hack the website of the Estonian Reform Party and placed an official apology (in Russian) as signed by Andrus Ansip, the Prime

Minister of Estonia at that time(Schmidt, 2013).On 9 and 10 May, attacks on government and private websites appeared to try to block communications between Estonia and the outside world, particularly Estonia's biggest pedestal, Hansabank, was targeted. On May 12 and 13, the volume of attacks subsided again. On May 14, there was a major attack on SEB Eesti hisbank, the second largest bank in Estonia, but by May 16 the volume of attacks had dropped to the same level on May 12 and 13. The raid finally died on 18 May. Altogether the raid lasted for twenty-two days(Tikk, Kaska, & Vihul, 2010).

Russian Cyber-Tactics

Russia was the party accused of being the main perpetrator of the cyber attack against Estonia. According to The Guardian media, this attack was caused by disagreements between Russia and Estonia about the removal of the bronze statue of soldiers in Tallinn which was a Soviet relic in Estonia. Because it was known that Estonia was a former part of the Soviet Union which at the end of the cold war was only able to liberate itself again from Soviet shackles. One of the valuable Soviet relics, namely the bronze statue of soldiers in Tallinn, was an important relic for Russia, especially for the communist movement there. So that the policy of moving the statue was accused of making Russia angry and forced to take threats against Estonia(Traynor, 2007).

With advances in technology, Russia was no longer relying on conventional capabilities to carry out attacks against Estonia. Plus the supporting factor for Russia to launch cyber-tactics against Estonia, which was a country that uses internet access effectively in all aspects of its state life. So that in carrying out "revenge" attacks against Estonia, Russia uses cyber-tactics or cyber tactics, namely the use of cyber media to attack Estonia to achieve Russia's strategic goal, namely to weaken the credibility of the Estonian government(Herzog, 2011).The purpose of a DDoS attack is to make use of the network impossible for internal or external users. In carrying out cyber attacks, Russia uses cyber-tactics using DdoS(Schmidt, 2013). DDoS attack or Distributed Denial of Service attack is an attack attempt to make a computer or server unable to work properly. This attack can cause server or computer performance to be very slow. That's because there are thousands of system spams that attack simultaneously. Besides DDoS attacks also disrupt communication between a host and its clients in various ways, this attack also allows changes that can cause damage to the system. This DDoS attack is the most frequent attack in cyber attack efforts. DDoS attacks against countries were previously known to have been used to attack the CIA.gov site, which was the work of a 12-year-old British hacker(Kemp, 2011).

Russia was also known to use cyber-tactics, web defacement, the use of web defacement is almost similar to DDoS. In carrying out the action, Russia was suspected of using the application ping floods to Botnets to spread spam (spamming). Botnets are malicious applications that can cooperate with DDoS attacks by creating and spreading millions of cyber zombies(Herzog, 2011).The DDoS attack and web defacement used by Russia attempted to weaken the network connection of all computers in Estonia. This aims to paralyze the state's activities. Cyber-tactics carried out by Russia impacted all activities of Estonian society and government for twenty-two days. Important sites such as banks, parliaments, ministries, newspapers and broadcasters are the main targets for hacking Russian hackers. These sites are the main targets because they are the most strategic sites to cripple the Estonian state(Schmidt, 2013).

Response from Estonia and NATO

In dealing with the threat of cyber attacks, Estonia has taken several repressive measures independently and in cooperation with international organizations. In Estonia's efforts to strengthen its defense and deal with threats that attack its country, Jaak Aaviksoo who was Estonia's Defense Minister at the time declared baseless accusations against the Kremlin and this could not be proven by Estonia and even NATO. Thus, Estonia can only act by issuing policies to improve cybersecurity protection and response protocols(Bright, 2007). The Estonian government also took repressive measures by blocking the entire .ru domain which is the domain of the Russian state which was the center of the attack. The Estonian government even had a chance to counterattack by launching a defacement attack on the Russian government's website by labeling it "Proud to be Estonian!" and "Estonia Forever"(Bright, 2007).

In dealing with cases of cyber attacks against their country, as a member of NATO, Estonia takes advantage of its membership by asking for help against the strongest defense alliance in the world. But before that, Estonia also asked for help from the Terena organization and other organizations working in cyber, research and defense. Assistance against attacks also came from Computer Security Incident Response Teams (CSIRSTs) based in several countries. CSIRTs have successfully restored the Estonian government and public service website in early May(Herzog, 2011).Together with NATO, Estonia was trying to find a way out by building a strong wall of cyber-security defense. At that time, it could be said that NATO was actually not ready to tackle the problem. This was because the cyber attack that occurred in Estonia in 2007 was the first and largest cyber attack against the country in history. So in response to this case, NATO's efforts are to call the Defense Ministers of member countries to gather and discuss recommendations for solving problems(e-Estonia, 2017).

The results of these negotiations resulted in several legal regulations regarding cyber crime, which were called the Tallinn Manual on the International Law Applicable to Cyber Warfare. The Tallinn Manual contains approximately ninety written laws on cybercrime. And in May 2008 the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) was formed. CCDCOE was engaged in shaping the cyber defense policies of NATO members. The CCDCOE also conducts large-scale cyber-defense exercises, although it is not technically an operational NATO unit. CCDCOE was a concrete manifestation of how a threat can form a very effective defense agency to deal with and prevent the possibility of a threat from occurring in the future(Gjelten, 2011).The 2007 cyber attack made Estonia the country with the strongest cyber defense and security in the world. Estonia becomes a reference for other developed countries to provide advice on the development of their country's cyber defense. In Estonia itself, several startups and companies have emerged, such as BHC Laboratory, Clarified Security, Bytelife, GuardTime, Cybernetica and others(e-Estonia, 2017).

Lesson Learned for Indonesia

Indonesia is one of developing country in South-East Asia that has major dependecy for internet. It is not to mention the advantage for the development of the country, as the majority of the population has now become more educated as internet offers various facilities for the citizen. But it’s also become trap for some cases, as internet now has become one of the most possible threatening warfare in the 4.0 industrial revolution era. Hybrid warfare is a threat where in addition to Regular Military Forces and Special Forces it also involves Irregular Forces, namely information and propaganda wars, diplomatic wars, cyber attacks and wars for economic domination. In Act No. 3 of 2002 ofRepublic of Indonesia National Defense Law, it has been stipulated that threats in the national defense system consist of military threats and non-military threats, including cyber threats(PINDAD, 2021).

As recorded by Indonesia Security Incident Response Team on Internet Infrastructure (IDSIRTII), there were atleast 48.8 million Internet attacks throughout 2015 in Indonesia(ID-SIRTII/CC, 2015). The high number of crimes and hackers in the Internet sector is a threat amid the massive growth of internet users in Indonesia. The cyber attacks threaten various sectors including Public Service, Economy, Defense, Security, and Energy. And in 2019, the National Cyber and Crypto Agency Indonesia (BSSN) reported 290 million cases of cyber attacks. This amount is 25% more than the previous year when cybercrimes caused US$ 34.2 billion in losses in Indonesia. The Covid-19 pandemic, in addition to triggering a significant increase in phishing attacks, spams and ransomware attacks, has also increased the pressure to establish a well-functioning cybersecurity infrastructure(CIPS Indonesia, 2021).

Minor cyber attacks caused by hackers should become alarm for Indonesia. This should awake Indonesia for the more major cyberattacks that could possibly happen in the future. The efforts that should be done by the Governments include, strenghtening its cyber security through better cyber defense such as better education for citizen for any privacy limitation shared through internet, strenghtening institutions that has authority for cyber security, involving the private sectors that have cyber security great potential in any cyber defense or security policy-making for securing better cyber in Indonesia.As the part and one of the leaders of

ASEAN, Indonesia should also consider to conduct talks and meetings withmember countries in order to create better cyber security for the region. This is not only an effort to bring togetherness of the member countries in the region, but also to prevent cyber war between member countries.

The Estonia cyber attacks in 2007 might be 15 years ago, but this attacks should and must be the great alarm for Indonesia to raise the awareness against any attacks and threats from the internet. Considering that the cyber attack that occurred in Estonia was a cyber war occured between countries and disabled vital activities throughout countries. Because cyber defense knows no country's territorial borders, attacks can come from within or from outside.

IV. Conclusion

The Estonian cyberattack in 2007 was the first cyberattack in the world. This shocked the Estonian citizens and Government for twenty two full days they could not carry out their activities which depend on internet access and computer network. In this attack Russia became the main unpredictable. There are indications that Russia can be seen in the country's response to allegations of Estonian cyber threats. The inconsistent response issued by Russia can be concluded that Russia is trying to avoid and cover up its involvement in this case. In carrying out the attack, Russia used cyber-tactics called a DDoS attack or Distributed Denial of Service attack. The use of DDoS is characterized by the large amount of spam generated by and slows down the computer. Estonia was helped by NATO to fight against the attackers to solve the case. NATO and Estonia then agreed to create *NATO Cooperative Cyber Defence Center of Excellence* (CCDCOE) which is by far the strongest cyber-defense cooperation in the world.

The cyber attack that occurred in Estonia in 2007 has become a lesson for the whole countries in the world, including Indonesia. As recorded by the authorities, Indonesia has a big potential for the threats coming from cyber platform. It was also mentioned by the Indonesia Governmental Law (Act No. 3 of 2002 ofRepublic of Indonesia National Defense Law), that Indonesia has to face two major source of threats coming from Military and Non-Military threats, including cyberattacks and cyberwar. Therefore, Indonesia should reflect more from the Estonia Cyber Attack in 2007 for better alarm to upgrade the better cybersecurity for the country. As the member of ASEAN, Indonesia should also become leader to raise joint awareness of cyber attacks as it is beneficial for both the region and member countries in South-East Asian. Because cyber defense knows no country's territorial borders, attacks can come from within or from outside.

References

[1.] Bright, A. (2007, May 17). *NATO is investigating siege on Estonian government, media, and banking websites, but Russia denies involvement.* Retrieved from The Christian Science Monitor: https://www.csmonitor.com/2007/0517/p99s01-duts.html

[2.] CIPS Indonesia. (2021, July 10). *Ringkasan Kebijakan | Perlindungan Keamanan Siber di Indonesia*. Retrieved from CIPS Indonesia: https://id.cips-indonesia.org/post/ringkasan-kebijakan-perlindungan-keamanan-siber-di-indonesia

[3.] e-Estonia. (2017, June 14). *How Estonia became a global heavyweight in cyber security*. Retrieved from e-Estonia: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

[4.] Fry, R. (2010, July 21). *Fighting Wars in Cyberspace*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/SB10001424052748703724104575379343636553602

[5.] Gjelten, T. (2011, January 4). *Volunteer Cyber Army Emerges in Estonia*. Retrieved from National Public Radio: https://www.npr.org/2011/01/04/132634099/in-estonia-volunteer-cyber-army-defends-nation

[6.] Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 49-60.

[7.] ID-SIRTII/CC. (2015). *Security News*. Retrieved from ID-SIRTII/CC: https://idsirtii.or.id/securitynews/index/270.html

[8.] Kemp, D. (2011, June 21). *British teen arrested over CIA, US Senate hacking*. Retrieved from Phys: https://phys.org/news/2011-06-british-teen-lulz-hacking.html

[9.] Lin, W., & Tom, C. (2016, April 14). *Financial Weapons of War*. Retrieved from SSRN: ssrn.com

[10.] McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. Retrieved from BBC: https://www.bbc.com/news/39655415

[11.] PINDAD. (2021). *Cyber Security*. Retrieved from PINDAD: https://pindad.com/cyber-security

[12.] Psaila, S. B. (2011, May 2). *Right to access the Internet: the countries and the laws that proclaim it*. Retrieved from Diplo: https://www.diplomacy.edu/blog/right-to-access-the-internet-countries-and-laws-proclaim-it/

[13.] Schmidt, A. (2013). The Estonian Cyberattacks. In J. Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (pp. 175-184). Morrisville: Cyber Conflict Studies Association.

[14.] The Economist. (2010, July 1st). *War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?* Retrieved from The Economist: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

[15.] Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations.* Tallinn: CCD COE Publications.

[16.] Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia*. Retrieved from The Guardian: https://www.theguardian.com/world/2007/may/17/topstories3.russia

[17.] X-Road. (2019, October 11). *X-ROAD® DATA EXCHANGE LAYER*. Retrieved from X-Road: https://x-road.global/

[18.] Zahra, I. (2021). THE BEGINNING OF THE INTERNATIONAL HUMANITARIAN LAW APPLICATION TO CYBER ATTACK: THE STATUS OF RULE 30 TALLINN MANUAL 1.0. *Padjajaran Journal of International Law*, 98-113.