DEVIANCE JURNAL KRIMINOLOGI
Volume 7 Nomor 1 Juni 2023
Hal: 32-45
DOI: http://dx.doi.org/10.36080/djk.2412

Blockchain Technology: Cyber Security Strategy in Post-2007 Cyber-Attacks Estonia

Dita Aulia Salma[1], Fahlesa Munabari[2]
[1]International Relations Department, Faculty of Humanities, President University
[2]International Relations Department, Faculty of Social Sciences and Global Studies, Universitas Budi Luhur
[1]Bekasi, [2]Jakarta, Indonesia
fahlesa.munabari@budiluhur.ac.id

Abstract: This article analyzes how blockchain technology became one of Estonia's cybersecurity strategies after cyberattacks against Estonia that occurred in 2007. As a result of these attacks, Estonia was able to significantly strengthen its cybersecurity. The article analyzes Estonia's steps to deal with cyberattacks in 2007 and the strategies used as anticipatory measures in preventing similar attacks in the future. This article also analyzes the use of blockchain technology in Estonia after the cyber-attacks in 2007. This study uses the offense-defense theory often known as the security dilemma theory, which contends that big war may be avoided when the defence has the upper hand over the offense. This article argues that the use of blockchain technology has not only strengthened Estonia's cybersecurity, but also been a counterbalance to the power of cybersecurity for Estonia's European neighbors, including Russia.

Keywords: Estonia; Blockchain Technology; Cyber Security; Russia; Cyber-Attacks

Abstrak: Artikel ini menganalisis bagaimana teknologi blockchain menjadi salah satu strategi keamanan siber Estonia setelah serangan siber yang terjadi pada tahun 2007. Akibat serangan tersebut, Estonia berhasil memperkuat keamanan sibernya secara signifikan. Artikel ini menganalisis langkah-langkah Estonia untuk menangani serangan siber pada tahun 2007 tersebut serta strategi yang digunakan sebagai langkah antisipasi dalam pencegahan serangan serupa di masa depan. Artikel ini juga menganalisis penggunaan teknologi blockchain di Estonia pasca serangan siber pada tahun 2007 Penelitian ini menggunakan teori ofensif-defensif yang sering disebut sebagai teori dilema keamanan yang berpendapat bahwa perang besar dapat dihindari ketika aspek pertahanan lebih unggul daripada aspek serangan. Artikel ini berargumen bahwa penggunaan teknologi blockhain tersebut tidak saja memperkuat Estonia keamanan sibernya, tetapi juga menjadi penyeimbang kekuatan keamanan siber bagi negara-negara tetangga Estonia di Eropa, termasuk Rusia.

Kata kunci: Estonia; Teknologi Blockhain; Keamanan Siber; Rusia; Serangan Siber

Introduction

In 2007, from 27 April to 18 May, cyber-attacks took place in Estonia for 22 days. This cyber-attack series targeted Estonian organizations' websites, including the

Estonian parliament, the Estonian banking system, broadcasters, police, and state departments. In this cyber-attack, Estonia believes that Russia is the main mastermind behind the attack amid the country's dispute with Russia over the relocation of the Tallinn Bronze Soldiers. The statue or memorial known as The Bronze Soldier of Tallinn is a form of respect and commemorates the contribution of the Soviet Union's Red Army, who fought against Nazi Germany in World War II. The Bronze Soldiers that had been stationed there by the former Soviet Union were set to be relocated by the Estonian government in 2007. It is believed that the Estonian government discriminated against the majority of people when it moved the Bronze Soldier statue from downtown Tallinn to the countryside. Estonia was thought to have disrespected the Red Army's role in the fight against Nazi Germany during World War II and ruined Soviet cultural heritage due to this policy.

Many ethnic Estonians regard the Bronze Soldiers in the city center as a symbol of Soviet occupation and oppression. Russian residents protested this policy on the sidewalk in front of the Estonian embassy on the 26th and 27th of April 2007. The incident was dubbed the "Bronze Night". Russian ethnic minorities in Estonia were part of this incident. Following this incident, the websites of the Prime Minister of Estonia, the websites of the Estonian Parliament, and the websites of political parties, banks, and the media were subjected to cyber-attacks, which began on 27 April 2007 (Mangelin, 2011). 800 people were detained in the capital city of Estonia as a result of this attack, which is believed to have left one person dead, 153 injured, and the Estonian system of government was paralyzed for around two weeks (Rolski, 2007).

The cyberattacks resulted in varying degrees of entropy[1] increases. Particularly Distributed Denial-of-Service (DDoS) attacks,[2] which obstruct government and civil society operations, creating a stream of adverse information about the Estonian organization and jeopardizing its capacity to operate effectively. The country's independence and capacity to look after and virtually defend itself is compromised by these assaults. Even though there is no physical harm to people or property, the attacks still amount to an act of informational aggression against Estonian businesses (Haataja, 2017, p. 165).

Only specific entropy types that involve an entity's material destruction or degradation are subject to legal regulation. Cyberattacks would more readily meet the legal definition of violence and be seen as a use of force under current law if they directly result in hardware damage or human injury. If this is not the case, the

[1] In computing, entropy is the randomness collected by an operating system or application for use in cryptography or other uses that require random data.
[2] Distributed Denial-of-Service (DDoS) is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

principles of non-intervention is to be applied, which effectively classifies the occurrence as non-violent below the level at which force may be used. The information approach, however, offers a way beyond legal ontological limitations that enable the recognition of non-material cyberattacks as a form of violence. A larger range of ontological violence can be recognized and restrained by law, for instance, through redefining violence via the concept of entropy and perceiving state entities in informational terms. On the other hand, despite popular perception, Estonia has not been the target of any particularly serious cyberattacks. However, political threats must be considered as aspects that could represent a major danger to cybersecurity. It is imperative to stress that a country can only achieve cybersecurity through an interconnected strategy that incorporates national policies, legal system, and the organization of actors. Reviewing Estonia's strategic, legal, and/or organizational developments after the 2007 hacks will help produces better anticipation to future cyber-attacks (Czosseck et al., 2011, p. 27).

All NATO-affiliated western allies urgently review the Estonian cyberattack and its ramifications. NATO has dispatched several experts in the field to Tallinn to look into the matter and assist Estonia in strengthening its cyber defense. Officials from Estonia said that one of the perpetrators of this cyberattack was from Russia and was connected to the Russian security services based on his online alias. A Finnish analyst, Mikko Hyppoenen, told the Helsingin Sanomat newspaper that it would be impossible to establish Russian official responsibility and that, if it so desired, the Kremlin could cause much more significant cyber damage (Traynor, 2007). Officials from the EU and NATO are cautious not to accuse Russia explicitly even if they want to bring up the problem with the Russian government. NATO does not consider this to be a military strike, but it needs to be handled quickly.

The attack on Estonia would inspire international copycat organizations in the future, and the circumstances of spring 2007 have given nations crucial knowledge for the advancement and improvement of their cyberwarfare capabilities. Although the information era has many advantages, it has also brought about new dangers, including international cyberterrorism and information warfare. The attack on Estonia demonstrates that even NATO Article 5 and the U.S. nuclear umbrella guaranty cannot ensure the security of a nation's sovereignty in cyberspace in the era of the so-called IT-driven globalization. Democracies must figure out how to strike a compromise between keeping effective early warning and monitoring systems and permitting Internet freedom. The Estonian cyberterrorism case demonstrates the need for the nation's foreign and security policy to evolve, adjusting to the rapid changing nature of the information technology’s sphere (Herzog, 2011, p. 51). The cyber defense plan for NATO has undergone a significant modification since the hack on Estonia. As a result of its lessons learned, the Alliance has enhanced its ability to react quickly and its policy procedures. While

some concerns still need to be resolved, the current legal and defensive frameworks are usually enough to safeguard NATO networks and support the Allied cyber defense authorities as well as the cyber defense agencies to improve information sharing and reaction coordination. Currently, NATO's cyber defense policy provides the Alliance with the guidance it needs to respond to cyberattacks, but the effectiveness of this policy depends on how well it is implemented. Therefore, NATO must ensure that its members and partners follow its cyber strategy (Joubert, 2012, p. 11).

The above review of literature discussed the conditions of Estonia after experiencing a cyber-attack in 2007. Starting from the side of NATO, what lessons can be learned from it, then how does International Law view the incident from an informational and legal approach, strategic and organizational changes in cyber security to the existing cyber policy after the incident of the cyberattack? Up to the present, however, there is still little literature that examines the topic of research seen from the analysis of the theory of offense-defense. Some are almost similar, many of which discussed the losses suffered by Estonia after the cyber-attacks. These studies looked at the responses of Estonia to the cyber-attacks and discussed the relationship between Russia and Estonia after the creation of a cyber defense policy by Estonia. It can also be inferred that it is difficult to prove who is to blame for the cyber-attacks. It is challenging to articulate how international law can be used to regulate cyberwarfare. It later produced the Tallinn Manual, a textbook created by the NATO-affiliated Cooperative Cyber Defense Center of Excellence (CCDCoE), which is situated in Tallinn, the capital of Estonia (Ranger, 2018, p. 9). Because escalation frequently happens when the laws are unclear and leaders respond, the assumption is that by making the law around cyberwarfare clearer, there will be less risk of an assault. Therefore, the middle way that can be taken by Estonia in responding to this problem is to strengthen its cyber security. Many technologies were built to strengthen cyber security and to make life easier for Estonians. Estonia is digital all over and well known as Blockchain Pioneer. This cyber-attack, which many concluded that Russia was the perpetrator, is a warning to Estonia. It has invested heavily in the development and use of digital infrastructure to consider more carefully the security implications of the technology they deploy. It also paved the way for the use of blockchain technology. This article attempts to answer how the blockchain technology became Estonian cybersecurity strategy to respond to the Estonia's cyber-attacks in 2007. It argues that having experienced from the massive cyber-attacks in 2007, Estonia developed the blockchain technology that is believed to be the appropriate solution to strengthen its cybersecurity.

Methods

The type of data indicates that the research methodology utilized in this article is a qualitative technique. What is meant by qualitative research is specifically a study that aims to comprehend the phenomena of what is experienced by research subjects holistically, through descriptions in the form of words and language, in a particular natural setting, and by applying a variety of scientific methods (Neuman, 2006). This article uses methods for gathering data from literature reviews of dictionaries, reports, magazines, journals, and other materials pertinent to the topic of study. These data are then collected, sorted out, verified, and analyzed using the theory employed in this study. This study uses the offense-defense theory to analyze the aforementioned data. This theory illustrates how efforts taken by one country to strengthen its security may have an adverse effect on other countries' security or may even be seen as weakening their own security. The ofence-defence theory, often known as the security dilemma theory, is a rather openly optimistic theory of international politics since it contends that big war may be avoided when the defence has the upper hand over the offense (Jervis, 1978, p. 171; Van Evera, 1998, p. 17). This article positions Estonia as a defender in the 2012-2018 timeframe that is the time after the cyber-attack in 2007 This theory helps the authors better understand how the collected data are relevant to and helps answer the research question posed in this study.

Results and Discussion

Estonia’s Cyber Attack in 2007

Estonia is the most northern of the three Baltic countries and is in northeastern Europe. Estonian has linguistic ties to Finland. Throughout a large portion of its history, Estonia has been ruled by foreign nations. It became a member republic of the USSR as one of its component republics in 1940. Especially in the border regions, Estonia is one of several nations that were formerly under the control of the Soviet Union. There, Russians live and work. The influence of Russian TV, Russian politics, and Russian culture is still very strong in Estonia even though many people have lived there their whole lives (FUKUHARA, n.d.). Relationships between Estonia and Russia, which had never been great since 1991, reached a new low in 2007. The siege of the Estonian Embassy in Moscow by Russia's pro-Kremlin youth movement allows it to be cited as an illegal breach of diplomatic law involving the embassy, such as the crisis of Tehran hostages 1979– 1981 (Liik, 2007, p. 72).

The two nights of rioting in Tallinn, the cyberattacks, and the verbal battle between Tallinn and Moscow make this the largest foreign crisis Estonia has faced since regaining independence in 1991. Its underlying roots appear to be that a controversial Soviet statue has been removed by the Estonian government on grounds of domestic politics, which angered local Russians and put up a fight with

Moscow. As a result, Moscow lost its moral compass through excessive resistance. The removed statue serves as a memorial to many of the ancestors of those who lost their lives in the World Wars (Liik, 2007, p. 75). Many of them disapproved of the pro-Soviet sentiment, and many of them understood why the statue bothered Estonians. However, the method of removing the statue was ambiguous and the government did not provide any serious justification for the act, which was what local Russians were demanding.

The biggest weakness of the Estonian government is that the whole migration procedure is seen as a technical and bureaucratic process. While every effort is made to ensure that everything is legal. There had been no attempt made to change the hearts and minds of the Russians (Liik, 2008). Estonia has long believed that native Russian speakers learn Estonian in the hope that they will be able to understand Estonian culture, history, and concerns about Russia. However, this is wrong. Efforts to change the hearts and minds also need to assimilate ethnic Russians with Estonians (Liik, 2007, p. 72).

Components of Estonia's Internet infrastructure were targeted by DDoS assaults, website hacking, DNS server attacks, bulk emailing, and comments spam over three weeks from April 27 to May 18, 2007. Estonian companies had a system crash at around 10 p.m. due to abnormally heavy data traffic. The website experienced web crashes. More spam and fraudulent emails in mailboxes. Attacks started with political institutions as their objective. Andrus Ansip, the prime minister of Estonia, and other well-known politicians received spams. The email system for the Estonian parliament had to be briefly shut down because it could no longer manage the exceptional volume of data. Postimees Online, an Estonian news organization, had to shut off foreign access to its network after being the target of two DDoS attacks on its servers, which restricted the ability of Estonians to make their voices heard overseas. Additionally, the Prime Minister is disparaged and insulted in the discussion area on Postimees Online by bots (Schmidt, 2013, p. 177).

The Estonian security community was not shocked by the attack. They believe that when there are riots in the streets, people will flock to the internet. However, the idea that a cyber-attack is imminent is not only based on intuition. The Estonian and global Internet security communities heard the message. A DDoS attack against an Estonian pillar of civic organizations was discussed by commenters in a Russian language forum in the mid of April 2007. Technical operators in Estonia quickly realized that the websites of numerous regional institutions had been the target of a DDoS attack due to their inability to centrally monitor national Internet services. The Estonian Ministry of Defense's head of public relations announced at around 1 p.m. on the 28th of April 2007 that "We are under cyber-attack," three hours later, a national security crisis had developed. DDoS attacks were practically a daily

occurrence. Jaak Aaviksso, the Defense Minister of Estonia, stated, "It appears that this is a national security problem" (Schmidt, 2013, p. 179).

For two reasons, the 2007 Estonian cyberattack constituted a turning point in the development of Internet security. First, these attacks gave the public the impression that cyberattacks can be a weapon in multilateral or bilateral confrontations(Iasiello, 2013, p. 3). Whatever the responses, the attack was consistent with the larger foreign policy plan the Russians had created to control their neighbors at the time. The Kremlin's tougher stance and desire to extend its cultural, political, and economic influence in nations bordering Russia's western borders were indicators of this. In line with its Western allies, Estonia's political response is to prevent Russia and other countries from attempting any additional deployments of assaults against civilian Internet infrastructure in other states. There have been many distinct policy frameworks employed. Government representatives criticized these actions as being inconsistent with international norms. The long-term objective is to lessen the amount of unpleasant online behavior that may be considered criminal. Since then, governments have worked to enhance awareness of and readiness for attacks on the operational technology side. Estonia and its Western security allies have raised the stakes and potential sanctions for adversaries who permit or even use volunteer organizations to target foreign Internet infrastructure by promising reciprocal assistance in the event of future significant attacks on national Internet and communication technology infrastructure (Ashmore, 2009, p. 7).

Russia's cultural and political influence in Estonia has diminished while Estonia has become more enmeshed in Western security and policy institutions. In history, the Estonian cyberattack will be remembered as the only time the defense minister proclaimed that the country was in a "national security scenario." The reaction to the attack in Estonia was a great success for the concepts of open information sharing and loose governance in the technical security community trust and ad hoc collaboration made possible by technology. As a result, the community of Cyber Defense League was formalized as a legal entity; in addition, the informal core group of response teams now serves as a formalized technical advisory body to the Estonian National Security Council; and the host organization for CERT, RIA, was granted special executive rights for upcoming national security situations (Jurkynas, 2014, p. 116).

Blockchain Technology as Estonia's Cybersecurity Strategy

From the above explanation, it is known that one of the factors that influence the state to behave in offense or defense is the technology factor. Since 2012, blockchain has been used in Estonia's governmental and private sectors to protect national data, e-services, and smart gadgets. The 2007 cyber-attacks lesson brings

up a challenge to Estonia. Estonia is challenged to demonstrate the authenticity and provenance of the human or machine of any electronic data assets without relying on centralized trust authorities. From here, Estonia started reforming its security system with various steps being taken. The Estonian cybersecurity plan is based on a cybersecurity strategy, which is also a component of the overall Estonian security strategy (Heller, 2017a; Ølnes & Jansen, 2018).

Estonia's Response to 2007 Cyber-Attacks

In playing its role as a defender, Estonia has been recorded as having done many things for both its country and the outside world in the cyber world. Quick steps began to be compiled by Estonia. The Estonian Information Systems Authority (Riigi Infosüsteemi Amet/RIA) has been given more authority and funding to oversee the security of information systems and regulate the protection of the country's information and communication infrastructure. The Critical Information Infrastructure Protection Department (CIIP) was established within RIA to regulate infrastructure protection (Czosseck et al., 2011, p. 27). The CIIP Commission was formed in 2011 to encourage public-private collaboration. The purpose of the commission is to exchange operational data, pinpoint problems, and develop solutions to strengthen the cyber security of the country's critical infrastructure. In addition, in 2013, a public-private collaboration project started to enhance smartphone users' skills and vendors' understanding of security issues.

Estonia views cybersecurity as an important component of overall security aimed at safeguarding the digital ways of life. The Estonian cyber defense strategy is structured around four main pillars, including upgrading information security skills, establishing national policies, and sustaining existing institutions to enable effective allocation of tasks in inter-agency collaboration. National defense was strengthened by the establishment of the Estonian Defense League's Cyber Unit (EDL CU), which was the result of cooperation between the government, private sectors, and third parties. EDL CU is used to enhance the security of Estonian business information systems (Shackelford, 2009, p. 33).

Estonia's sense of insecurity makes them prepare everything. Estonia feels that education is the main source of training and awareness-building in cyber security, so they think the information technology foundation is the best investment. Estonia's response to the 2007 cyberattacks included not only developing cyber skills training and implementing cyber security curricula in schools and colleges but also raises cyber issues in international forums. This is important in economic affairs and international relations to work with NATO and the European Union to build a stronger security defense supported by many countries. Significantly, the Warsaw Summit identified cybersecurity as one of NATO's focus areas (Joubert, 2012, p. 31).

NATO has selected Estonia to host the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), which was housed in the Estonian Training and Development Center for Defense Forces Information and Communication Systems. Estonia has created its national action plan against cybercrimes (SIVAK) (Herzog, 2011, p. 53). Germany, Italy, Spain, and Latvia have each pledged their support, along with additional European countries. Representatives from the U.S. also participated in the conference in Tallinn. The creation of institutions such as the Estonian Cyber Security Plan, established in May 2008, allows the formulation of an Estonian cyber defense strategy. The defense strategy is created by a multi-agency council under the direction of the Minister of Defense, Jaak Aaviksoo. (Haataja, 2017, p. 170). Estonia's self-defense can be seen from its initiative in creating defense strategies due to its experienced training in cyber warfare techniques. Estonia has also started offering formal courses in cybersecurity. For Estonia, international cooperation is very important. Given how dependent the Estonian economy is on other countries, one of the strategies to attack Estonia is to attack countries that depend on Estonia. Therefore, Estonia invites other countries to improve their respective country's cyber security (Areng, 2014, p. 11).

Blockchain Technology in Estonia

Estonia started testing the technology in 2008 even before the Bitcoin white paper that first coined the term “blockchain” was published. In Estonia, the use of real-world blockchain technology, called KSI (Keyless Signature Infrastructure), has been successfully applied to achieve the important goals of integrity and confidentiality of citizens' sensitive data as well as awareness of corrupt behavior and internal threat vectors. The fact that Estonia was the subject of a cyberattack in 2007 is one of the major factors contributing to its status as a blockchain leader. Blockchain technology was proposed as a solution in 2007 and officially adopted as the KSI blockchain in 2012, which was managed by the private Estonian company called Guardtime. Additionally, Guardtime performs similar work for NATO and the US government (Heston, 2017, p. 5).

In 2008, the Estonian government started experimenting with and testing this new technology even before Satoshi published his white paper. Currently, the term blockchain has not been coined, and Estonians refer to it as a "hash-linked timestamp". Since 2012, hash-related time-tagging, or blockchain, has been used operationally in many Estonian registries, such as the national health code, judiciary, legislative, security, and commercial systems. Nearly all public services in Estonia are digitized and accessed through a secure digital identity assigned to every citizen and resident. Since early 2012, blockchain has been used in Estonian private medicine as well as cybersecurity.

Blockchain is a digital data bank storage system connected to cryptography. The goal of blockchain technology is to create a decentralized environment where no third-party controls transactions and data. Blockchain is closely related to cryptocurrency, which was launched by Satoshi Nakamoto. Satoshi Nakamoto is a pseudonym. He launched Bitcoin, that is, a cryptocurrency in 2008 and built a blockchain system to run it (Chatterjee & Chatterjee, 2017, p. 7).

In short, bitcoin is a digital currency. To run bitcoin in cyberspace, a security system is needed, therefore Satoshi built a security system called blockchain. Blockchain is a public ledger or digital ledger to ensure that every transaction that occurs uses valid bitcoin and that the movement of bitcoin is recorded. Regarding cryptography in this digital ledger, blockchain is connected to cryptography in its working system (Yli-Huumo et al., 2016, p. 19). Cryptography or cryptology are mathematical techniques related to information security. Cryptography is a field of study in mathematics and informatics. It is the key to the bitcoin technology, which makes digital money unforgtable. Digital money or cryptocurrency is the designation of bitcoin in this cyberspace. Thus, bitcoin is a digital currency that uses cryptography for its security. In other words, blockchain is a technology that is bigger than bitcoin, because many ordinary people understand blockchain as electronic money or digital money (Heller, 2017b, p. 53).

Blockchain technology may be viewed as a "digital defensive dust" that covers all the data and smart devices that need to be protected against corruption and misuse. One approach to consider it is as follows: every change to the data can be recognized right away based on traces left in the pattern of the "digital protection dust" that covers the data. The chain instantaneously reflects all modifications that do not match the mathematical code in the chain, which is made possible by blocks of "digital defensive dust" being connected and forming a chain that is scattered in millions of computers globally.

The use of blockchain technology in Estonia has the potential for saving millions of lives and conserve resources while preventing the loss or early detection of potentially sensitive data manipulation, such as that relating to health, intelligence, and legal records as well as smart devices such as medical equipment, military machinery, and self-driving cars. The KSI Blockchain has the benefit of being decentralized because there is no single server where all the data is kept. As a result, even if one node in the network fails, the system can still function. Guardtime does this by dispersing its server clusters across the globe. This architecture nevertheless accomplishes the objective of lowering a single point of failure, although not being as completely decentralized as the bitcoin network (Scrutton & Mardiste, 2015).

Estonia uses blockchain technology to guarantee the accuracy of public data and systems. The Estonian Information Systems Authority (RIA), a vital service provider for the government, making sure that state Agencies have access to the blockchain network through the X-road infrastructure. State Gazette, Official State Announcements, Healthcare Registry, Property Registry, Business Registry, Succession Registry, and Digital Court System are just a few of the state registries that are enabled by blockchain technology. No data is ever stored on a blockchain. Instead, it works like a speed camera to record who, when, and how a law was broken. Every change to the data can be seen because it creates a mark in the pattern of the "digital defensive dust" that surrounds data protected by blockchain technology. The same blockchain technology employed by Estonia, KSI Blockchain by Guardtime, is currently utilized by NATO and the U.S. Department of Defense (Aaviksoo, 2019).

Since blockchain relies on many people's eyes to make it secure, it is evident that sensitive data should not be maintained there. The "hash values," which are effectively digital fingerprints of the original data, are what are stored on the blockchain to secure sensitive data. The same is true for digital fingerprints: while they uniquely represent the original data, it is impossible to infer anything about the data itself based on the "hash values," just like your own fingerprints uniquely identify you but do not reveal anything about your race, eye color, or thoughts. The blockchain, therefore, contains no original data, hence it makes no difference who accesses it (Jackson, 2013, p. 13).

That is how the blockchain improved Estonia's condition. Estonia is a pioneer of blockchain technology and has even become a digital republic. This shows that the strengthening of Estonia's cybersecurity strategy through blockchain was due to self-defense encouragement that has made Estonia feel insecure after the country was devastated by a cyber-attack in 2007. In addition, at that time Estonia could not blame anyone, other than the first case where there was no international law that it is also not clear who the perpetrators behind the cyber-attack were, even though all the evidence and most rational analysis pointed to Russia. Conditions like this drove Estonia to strengthen its national cyber security through the development of the blockchain technology that has a positive impact on aspects of its people's lives (Mahankali, 2019, p. 23).

Conclusion

The cyber-attack on Estonia in 2007 required Estonia to accept the consequences of information security collapse and it became a national emergency that disrupted many aspects. For about three weeks, the wheel of Estonian life was disrupted. The impact of this attack was massive even if we do not use a weapon. Evera's offense-

defense theory succeeded in explaining the case of the Estonian cybersecurity strategy after the cyber-attack (Van Evera, 1998). Of his ten hypotheses about the causes of the war, one of them can explain the cause of the Estonia's development of the blockchain technology. The variables in the theory are met and proven to show that Estonia is playing its role as a defender through a wider range of factors other than the military, namely technology. Estonia realizes that when a cyber-attack occurs, it is not a sudden thing, but the inability of the Estonian cyber security to deal with the DDOS attack has caused chaos in the country. This condition required Estonia to increase its cyber security and surveillance because this was the first thing that happened in the world at that time. There was no international law that regulated it. In addition, the perpetrators of this crime could not be proven even though the most rational evidence pointed to Russia. The way to prevent war from happening was to respond to the cyber-attack, Estonia as a defender implements tactics and initiatives aimed at long-term goals, which eventually became a blockchain pioneer.

This study argues that the blockchain technology is the appropriate solution for Estonia. The use of blockchain technology in Estonia makes Estonia secure and becomes a counterweight to foreign countries that threaten it because it has succeeded in demonstrating its strength in cyberspace (Mahankali, 2019). Blockchain development goes to a higher level while enabling greater consumer protection. While a fully decentralized future has not yet arrived, there is still a real role for legislators to play. This supports the offense-defense theory's central tenet that conflict can be averted if defense predominates or counterbalances offense's dominance (Van Evera, 1998, p. 35). The examination of this article demonstrates that the offense-defense theory can provide a comprehensive understanding of the reasons behind Estonia's aggressive behavior as well as the dynamics of security and defense in a specific area. This argument still holds true when analyzing state behavior in the context of global interactions.

References

Aaviksoo, A. (2019). Building blockchain powered trusted digital health services. Estonia. *Blockchain in Healthcare Today*.

Areng, L. (2014). Lilliputian states in digital affairs and cyber security. *The NATO Cooperative Cyber Defense Centre of Excellence Archive, Tallinn Paper Series*, *4*.

Ashmore, W. C. (2009). *Impact of alleged Russian cyber attacks*. ARMY COMMAND AND GENERAL STAFF COLL FORT LEAVENWORTH KS SCHOOL OF ADVANCED ….

Chatterjee, R., & Chatterjee, R. (2017). An overview of the emerging technology: Blockchain. *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*, 126–127.

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *1*(1), 24–34.

FUKUHARA, Y. (n.d.). *'We belong to Estonia': Influence of Russia's invasion of Ukraine on Russian speakers in Estonia*.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, *9*(2), 159–189.

Heller, N. (2017a). Estonia, the digital republic. *The New Yorker*, *18*.

Heller, N. (2017b). Estonia, the digital republic. *The New Yorker*, *18*.

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60.

Heston, T. (2017). *A case study in blockchain healthcare innovation*.

Iasiello, E. (2013). Cyber attack: A dull tool to shape foreign policy. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 1–18.

Jackson, C. M. (2013). Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success. *New Voices in Public Policy*, *7*(1).

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Joubert, V. (2012). *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* JSTOR.

Jurkynas, M. (2014). Security concerns of the Baltic States in the twenty-first century. In *Small States and International Security* (pp. 113–129). Routledge.

Liik, K. (2007). The "Bronze Year" of Estonia-Russia relations. *Estonian Ministry of Foreign Affairs Yearbook*, *2007*, 71–76.

Mahankali, S. (2019). *Blockchain: The Untold Story: From birth of Internet to future of Blockchain*. BPB Publications.

Manggalany, M. S. (2011, November 18). Babak Baru Serdadu Cyber di Estonia. *Viva News*.

Neuman, W. L. (2006). *Workbook for Neumann Social research methods: qualitative and quantitative approaches*. Allyn & Bacon.

Ølnes, S., & Jansen, A. (2018). Blockchain technology as infrastructure in public sector: an analytical framework. *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1–10.

Ranger, S. (2018). What is cyberwar? Everything you need to know about the frightening future of digital conflict. *Zdenet. Com, December*, *4*.

Rolski, T. (2007). Estonia: Ground Zero for World's First Cyber War?[Electronic Version]. *ABC News*.

Schmidt, A. (2013). The Estonian Cyberattacks. *A Fierce Domain: Conflict in Cyberspace*, *2012*, 174–193.

Scrutton, A., & Mardiste, D. (2015, December 4). With an Eye on Russia, Estonia Seeks Security in Computing Cloud. *Reuters*.

Shackelford, S. (2009). Estonia two-and-a-half years later: a progress report on combating cyber attacks. *Journal of Internet Law, Forthcoming*.

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, *17*(05).

Van Evera, S. (1998). Offense, defense, and the causes of war. *International Security*, *22*(4), 5–43.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS One*, *11*(10), e0163477.