Strengthening Digital Ecosystems for Sustainable Development in Indonesia: Anticipating Cyber Threats

To cite this article: Muhammad Syaroni Rofii 2020 IOP Conf. Ser.: Earth Environ. Sci. 436 012026

View the article online for updates and enhancements.
Strengthening Digital Ecosystems for Sustainable Development in Indonesia: Anticipating Cyber Threats

Muhammad Syaroni Rofii

1Graduate School of Strategic and Global Studies, University of Indonesia, Jalan Salemba Raya 4, Jakarta, Indonesia

E-mail: muhammadsyaroni@ui.ac.id

Abstract. The digital industry is experiencing rapid development in Indonesia. Indonesian local companies such as Gojek, Tokopedia, Bukalapak and Traveloka have now transformed into big companies and have high valuations which attract foreign direct investment. Considering the enormous opportunities of the digital industry, the Indonesian government itself has a vision to make digital industry and creative industry as supporting elements for sustainable development in Indonesia. In order to prepare a sustainable development ecosystem that has ability to survive, the Indonesian government needs to anticipate cyber threats which later pose a real threat to the industry. This article seeks to analyze the development of the digital industry in Indonesia and anticipation that can be done to prevent cyber threats. From this study the author found a number of facts that the damage and losses caused by cyber attacks are very massive so that preventive solutions are needed. This study uses a qualitative method by analyzing primary data from Bank Indonesia (BI) and the Financial Services Authority (OJK).

1. Introduction
The digital industry is experiencing rapid development in Indonesia. It is marked by the presence of startups from Indonesia which attract huge numbers of consumers. Some local companies that later became digital industry giants in Indonesia such as Gojek, Tokopedia, Bukalapak and Traveloka have succeeded in changing the lifestyle of Indonesian people who are familiar with the digital world. In addition to presenting applications that are easy to use, these startups have also begun to introduce the concept of using digital money which indirectly reduces the use of cash. In addition, the presence of digital-based companies helps create new jobs and increase economic transactions in the field of micro, small and medium enterprises. The growth of the new middle class is also part of the government strategy to achieve sustainable development goals.

The derivative of the digital industry which has recently become a trend in Indonesia implies to the increasing number of transactions using the internet and mobile phones. For example, Gopay which is a product of a Gojek company might be the first Indonesian company to successfully introduce the concept of using non-cash money to Indonesian people. Gojek riders are generally high school graduates with an average age of over 40. All Gojek riders are required to understand the Gopay concept because that way they can make transactions with users. In addition, the presence of Gopay has also changed the lifestyle of Indonesian people who were previously very dependent on vehicles, now only by using the application on cell phones, they can order food, order cleaning services, order tickets and to order any kind of products they want from home. Gofood for example, as an application for food orders is an application that is widely used by women. According to Gojek's Chief Commercial Expansion, Catherine Hindra Sutjahyo, that the value of Gofood transactions throughout 2018 reached 28 trillion rupiahs

Gopay itself is one of the products offered by Gojek to support transactions in the Gojek system. In addition to Gopay, companies engaged in the digital and e-commerce industries
generally utilize non-cash transactions as an effort to facilitate customers and keep up with the growing trends in society. This sector is often referred to as financial technology or fintech. Based on data released by the *Otoritas Jasa Keuangan* or Financial Services Authority (FSA), who are responsible for approving license and monitoring financial services activities noted that the number of financial technologies that have been officially registered as of August 2019 reached 127 companies[^2]. The trend of transaction between 2018 and 2019 increased significantly. For the category of loans (fintech lending) according to data in May 2019 it has reached 33.2 trillion, while for the category of payments or fintech payments has reached 47.1 trillion Rupiah[^3].

Indonesian government itself has formed the Financial Services Authority (OJK) which is tasked with granting licenses for the operations of a company engaged in financial services, besides that the OJK is also tasked with auditing every company engaged in the financial sector to comply with the conditions set by Indonesian government. In its development there is a tendency to increase the number of registering companies to obtain business licenses from OJK. This shows that fintech is a sector that needs the attention of the Indonesian government from various aspects, ranging from aspects of economic infrastructure to its resilience from disturbances and threats. So far, the Indonesian government, as conveyed by the Coordinating Ministry of Economy Darmin Nasution, said that the Indonesian government has concerns regarding potential losses created by misuse of customer data by companies, monopoly fintech businesses by a number of large companies and the use of fintech for money laundering activities.[^4]

The views expressed by the government show that the Indonesian government has not yet seen the potential of cyber threats to the fintech ecosystem in Indonesia. Seeing the above problem, this research seeks to analyze: how is the development of fintech in Indonesia and how is the potential of cyber threats to fintech business infrastructure in Indonesia? And what is the solution to that problem?

This article uses a qualitative research method to look at the development of fintech in Indonesia by analyzing the latest data in the last five years and then analyzed in depth with a descriptive analytic approach. The data used is taken from official data from government agencies and periodic reports related to financial transaction reports from the Financial Services Authority in Indonesia. The composition of this article begins with an introduction reviewing the development of the digital industry in Indonesia, then in the next section it is explained about the phenomenon of cyber attacks that threaten the industry, then in the final section it is explained about solutions that can be used to anticipate cyber attacks.

2. The Development of Financial Technology in Indonesia

As mentioned in the previous paragraph that the development of fintech received appreciation from the government, this was conveyed by the Coordinating Minister for Economic Affairs Darmin Nasution. The government also appealed to businesses to maximize the potential of fintech as a promising business sector in Indonesia. In addition, the government as a regulator seeks to anticipate that business actors who have been involved in fintech business are not monopolized by a small number of entrepreneurs who have the potential to create market monopolies that can harm customers, another anticipation conveyed by the government is the potential for misuse of fintech for conflicting activities with laws in Indonesia such as money laundering and misuse of customer data for corporate purposes[^5].

The view of the Indonesian government regarding the challenges faced by fintech in Indonesia shows that the government’s concern is still around the potential fraud committed by business actors as well as potential violations committed by business actors against the rules set
by the government. The government has not seen the aspect of cyber security as a major issue that deserves special attention. This view does not place the aspect of cyber security as a major issue may be caused by the lack of information supply to the Ministry of Finance and the Coordinating Ministry of Economy regarding the impact of damage and losses that could occur if a cyber-attack scenario occurs against fintech companies in Indonesia.

3. The Patterns of Cyber Attacks Toward Industry
The Indonesian public's perception of the threat of cyber is still low, because the Indonesian government has not made the issue of cyber attacks a threat that endangers the country's resilience. At the ASEAN region level, even though the issue of the potential for cyber attacks has not been much discussed by its leaders. For the ASEAN region the issue of cyber security is still not the main topic of leaders in the region, ASEAN leaders are still focused on the potential for traditional threats. Only Malaysia and Singapore are more prepared in mapping potential non-traditional threats in this case cyber threats.

The European Union and the NATO defense alliance, including organizations that have concerns about the growing trend of cyber threats to government and private sector information systems. In order to anticipate the changes that occur related to the potential threats arising from the development of information technology, NATO holds an annual meeting to discuss the issue of cyber security, which was attended by high-ranking officials of the NATO defense members. While the European Union, since 2013 has launched the EU Cyber Security Strategy, the European Security Agenda also places the issue of cyber security as a contemporary problem that must be faced. Richard A. Clarke as a White House security advisor in an interview with the Journal of International Affairs explained that cyber war targets sectors connected to the internet or referred to as the "Internet of Things", examples of installations that are often the target of attacks are public installations such as nuclear reactors connected to the internet system, machines that detect the survival of patients connected to information systems, gas pipelines that are also controlled via a computer. These examples are targeted targets of attackers, both carried out by state and non-state actors.

However, the statement made by Clarke as a US defense advisor can be seen as an effort to divert the issue based on the reality on the ground related to US involvement which is said to be involved in making the Stuxnet virus which is a weapon in the form of the first computer virus capable of crippling Iran's nuclear installations. Stuxnet itself is referred to as a computer virus created by the US which was later developed by Israel to make the Stuxnet virus very aggressive in attacking its targets. It must be admitted that the US, Israel, Britain, China, Russia, Iran, Syria, and North Korea are countries that have the ability to attack and defend successfully in cyber war. Each country has a special detachment to take care of the affairs of the cyber attack with different designations.

Using the example of the US, the US has a long history in the affairs of developing forces that work specifically to attack and ward off cyber attacks. Although each US president has his own characteristics and has different policies in matters of cyber war, they have strong fundamentals in designing their national defense buildings. President Ronald Reagan is known as the US president who has a very high concern regarding the issue of non-traditional attacks from US enemies by issuing a National Security Decision Directive-145 or NSDD-145 titled "National Policy on Telecommunications and Automated Information Systems Security".

The issuance of the decree was intended to anticipate attacks that were not as sophisticated as cross-continental missile attacks but had the same damage impact on national security. Another
US President George W. Bush also used the development of information technology to succeed the 2003 Iraq War military operations. Furthermore, President Barack Obama, although not giving broad discretion to the intelligence services to access information and conduct surveillance to US citizens because of consideration of civil liberties but behind screen, through Defense Secretary Robert Gates, the US formed the Cyber Comand (Cyber Command Center) which received a high enough budget allocation. In the first three years the agency received a budget of 2.7 billion dollars to 7 billion dollars (plus another 7 billion dollars for cyber activities in the military environment. While the number of US cyber troops increased from year to year, from 900 personnel to 4000 personnel, the latest data as mentioned by Fred Kaplan in his book, reaches 14,000 personnel [12].

The US itself has recently used many unconventional methods to conquer its targets, the NSA and the CIA as intelligence services were given a greater role to carry out operations in Iraq. Since 2007, for example, the US has sent more operators who understand computer systems and intelligence, while organic troops have been withdrawn because they consider the use of cyber war instruments to be more effective. Since 2007 the US, which was in control of operations held by David Petraeus, also opened a representative office in Iraq at Al Balad Air Base. With operations that maximize the role of information technology, the US succeeded in crippling four thousand Iraqi rebels. The rebel crackdown was greatly helped by a system known in the US military operations dictionary as the Real Time Regional Gateway [13].

Another case that shows the role of information technology in intelligence operations is when Israel carried out an operation called the Orchard Operation, in this operation the Israeli military F-16 fighter jet carried out an attack on a Syrian nuclear installation that was successfully built by North Korean scientists, Israeli military fighter jets succeeded in blowing up a Syrian nuclear installation without being noticed by the radar guards, behind the attack there was the role of Unit 8200 Israel who succeeded in breaking into the Syrian military radar system with a program known as Suter. Unit 8200 is known to have a successful track record in intelligence operations [14].

Likewise with the pattern of cyber attacks experienced by Estonia it is also very interesting to emphasize the existence of a cyber war involving the state. In April 2007 Estonia was the victim of a cyber attack allegedly coming from Russia. The cyber attack began with tensions triggered by anti-Russian sentiment delivered by the Estonian president who issued a policy of removing the bronze statues that stood in the city of Talin. Some groups in Estonia protested known as Bronze Night and vandalized the Russian monument, police tried to secure the statues in the city so that they would not continue to be the target of hatred which also triggered ethnic clashes. Not long ago Estonia had a barrage of cyber attacks targeting internet and telephone networks. Estonians had experienced difficulties because for three weeks they were unable to use telephone networks, bank accounts, credit cards, in addition to networks connected to parliament, ministries, government offices, shops, military communications were disrupted [15].

In addition, the incident that happened to Danish cargo company Maersk also became a real example of the existence of this cyber attack. That in 2017 Maersk engaged in the transportation of cargo ships across the country had suffered losses due to cyber attacks on their information systems. In 2017 Russian intelligence is said to be carrying out an attack on Ukraine by spreading the NotPetya virus. The virus attack on the information system of the European company made him suffer losses of up to 300 million dollars. This loss rate is caused by the death of the server and sending activity continues every 15 minutes. The attack from the Notpetya virus successfully paralyzed the Maersk company operating system and it took three days to be able to restore the system to its original shape [16]. Of course the loss will be even greater if the company
fails to stop the attack at an earlier time.

We imagine companies in Indonesia have not put security aspects in their company policies. It may be that the perception of the leader of a digital company from Indonesia about the threat is very agile because they feel Indonesia has no enemies with countries that are often involved in cyber warfare such as the United States, Russia, China and North Korea. Indonesia's position that has no history of hostility with countries that are often associated with cyber warfare may be a factor that makes the leadership of Indonesian companies have a perception that does not pay too much attention to the potential for cyber attacks.

4. Potential Cyber Threats

The higher the number of digital application users, it automatically increases the number of users who deposit their money in applications based on internet and server networks. The development of information technology can also be a source of threat to the state, in this case cyber attacks, the existence of cyber attacks is increasingly evident for now it is evidenced by attack data throughout 2018 and 2019 which show that the country is not silent, the state is directly involved in attack activities cyber, therefore Indonesia must also be active in mapping every potential attack for the sake of Indonesia's national security and resilience.

Even though cyber warfare is not really a priority for policy makers, the impact of cyber war is very real and directly touches people's lives. Cyber attacks that are controlled behind a monitor screen are able to turn off electricity in a city, cut off waterways, create riots, break into customer data, and trigger national destabilization, to name a few.

For this reason, it is never too late for the Indonesian government to respond to the development of cyber threats by mapping each potential attack and making improvements to the information system concerning the data of Indonesian citizens. In addition, the government also needs to maximize the role of the National Siberian Body and State Code to secure each sector that has the potential to be targeted by the attackers.

NATO in a document they released in 2012 mentioned anticipatory steps that could be taken by the government in order to respond to the emerging attack trends in cyberspace. There are at least four categories of threats that can jeopardize the national security of a country, first, the phenomenon of military cyber (cyber troop), that there is currently a real potential threat caused by the development of structured attacks by cyber troops driven by the state. A number of countries have actually launched virtual weapons to respond to this model war. Second, cyber crimes, cyber crime activities currently can endanger individuals and the state in the form of theft of individual or company data in the form of theft of intellectual property rights and confidential data from the banking sector. Third, Operation Intelligence, a contemporary intelligence operation carried out by the state, currently focuses on surveillance using artificial intelligence technology to monitor every movement in cyberspace. Fourth, cyber diplomacy, diplomacy today is not only focused on traditional instruments, diplomacy has developed very rapidly where the use of internet facilities is very dominant in helping the work of government in conducting public diplomacy [17].

Data released by the United States CSIS also shows the intensity of cyber attacks carried out by hackers sourced from countries that have so far been considered to have reliable cyber capabilities. Throughout 2018 to 2019, China, Iran, North Korea, Russia, the United Kingdom and the United States are among the categories of countries most frequently targeted for attacks and are suspected to be attackers in incidents in cyberspace. While the target of cyber attacks is mostly aimed at government agencies, government partners, technology companies, and companies engaged in the financial sector. The number of attacks that continues to increase shows a trend of
increasing state involvement in cyber attack activities. This is confirmed by the following data in Figure 1 [18].

![Figure 1. Cyber Attacks during 2016-2019](image)

5. Findings
From this research the author found the fact that the existence of cyber threats has the potential to disrupt the continuity of development in Indonesia. Indonesia's development vision that has undergone a transformation is directed from being previously dependent on natural resources to an economy based on ideas and creativity and supported by adaptation to technology. The emergence of e-commerce companies such as Bukalapak, Tokopedia, and Blibli shows where the Indonesian economy is heading. In addition, the emergence of Gojek's phenomenon has succeeded in transforming Indonesia's previously classic economic ecosystem into a very modern one. With the help of Gojek, micro, small and medium enterprises are able to reach the market quickly, thanks to Gojek's assistance, businesses in the field of food services are gaining new market segments from the new middle class who have a lifestyle of relying on cell phones and the internet to sustain their activities. The trend of using the internet to meet daily needs is an interesting phenomenon in Indonesia.

However, from this research it is found that the Indonesian government still does not see cyber war and cyber threat as an issue that needs serious attention. Whereas in the NATO alliance countries the issue of cybersecurity became the dominant topic at each of their meetings. Cases of cyber-attacks on companies in Europe and Indonesia have not been able to change the perception of the Indonesian government about the dangers of cyber-attacks on the sustainability of development based on digital ecosystems that depend on the internet.

References

[1] Republika, “Nilai Transaksi Gofood Tembus Rp 28 Triliun”, https://www.republika.co.id/berita/gaya-hidup/kuliner/19/02/20/pn7ykt368-nilai-transaksi-gofood-tembus-rp-28-triliun

[2] Perkembangan Fintech Lending, Available at:  https://www.ojk.go.id/id/kanal/iknb/data-
Development of Fintech in Indonesia, Available at: https://keuangan.kontan.co.id/news/continue-to-grow-following-challenges-developments-fintech-in-indonesia.

“Terus bertumbuh, berikut tantangan perkembangan fintech di Indonesia” Kontan https://keuangan.kontan.co.id/news/terus-bertumbuh-berikut-tantangan-perkembangan-fintech-di-indonesia.

Overview of Cybersecurity Status in ASEAN and the EU, Yaksha (2019). https://project-yaksha.eu/wp-content/uploads/2019/05/D1.1_Overview-of-Cybersecurity-Status-in-ASEAN-EU_VF.pdf.

NATO cyber security conference concludes after record attendance, Available at: https://www.ncia.nato.int/NewsRoom/Pages/20191017-NATO-cyber-security-conference-concludes-after-record-attendance.aspx.

Radoslav Repa, The Updated Cyber Landspace in the European Union for the Trusted Digital Single Market, https://www.osce.org/chairmanship/410360?download=true.

The Risk of Cyber War And Cyber Terrorism Author(s): Richard A. Clarke Source: Journal of International Affairs, Vol. 70, No. 1, The Cyber Issue (Winter 2016), pp. 179-181.

Stuxnet: The Real life Sci-fi Story of “the world’s first digital weapon”, www.abc.net.au, diakses 20/02/19.

National Security Decision Directive Number 145 “National Policy on Telecommunications and Automated Information Systems Security”, Available at: https://fas.org/irp/offdocs/nsdd145.htm.

Kaplan, Fred, Dark Territory: Secret History of Cyber War, New York: Simon and Schuster, 2016.

“Mission Creep: How The Nsa’s Game-Changing Targeting System Built For Iraq And Afghanistan Ended Up On The Mexico Border” available at: https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/.

“The Story of 'Operation Orchard', How Israel Destroyed Syria's Al Kibar Nuclear Reactor”, available at: https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Rain Ottis ‘Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective’, available at: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf; 2007 cyber attacks on Estonia, https://www.stratcomcoe.org/download/file/fid/80772

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million, Available at: https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#1bec71424f9a.

Moss, Jeff, et.all, “Cyber-security: The Vexed Question of Global Rules, An Independent Report on cyber-preparedness around the world”, Security Defense Agenda and McAfee Company, 2012.
[18] Significant Cyber Incidents, Available at: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.