NUANSA

JURNAL PENELITIAN ILMU SOSIAL DAN KEAGAMAAN ISLAM

P-ISSN: 1907-7211 | E-ISSN: 2442-8078

Volume 20 No. 1 January-June (2023)

Published By:
Research Institute and Community Engagement
State Islamic Institute of Madura

NUANSA

Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam

Vol. 20 No. 1 January-June (2023)

Nuansa: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam is a journal that publishes scientific articles which have been derivated from research on social sciences and islamic studies. This journal is published biannually on June and December and published articles reviewed by experts on the related issues.

Jurnal Nuansa's scope includes: education, culture, politics, law, economy, theology, philosophy, communication, and history.

All published articles will be added with a DOI CrossRef Unique Number

Nuansa: Jurnal Penelitian Ilmu Sosial dan Keagamaan Islam has been accredited by The Ministry of Research, Technology and Higher Education of the Republic of Indonesia as an academic journal in Sinta 3 (SK No.36/E/KPT/2019) valid for 5 years from Volume 16 No. 2 2019.

P-ISSN: 1907-7211
E-ISSN: 2442-8078

Editorial Office:
Nuansa: Jurnal Penelitian Ilmu Sosial dan keagamaan Islam, Research Institute and Community Engagement
of IAIN MADURA
Jl. Raya Panglegur KM. 4 Tlanakan Pamekasan, Jawa Timur, Indonesia, 69371
Email: jurnalnuansa@gmail.com
Website: http://ejournal.iainmadura.ac.id/index.php/nuansa

TABLE OF CONTENTS

nuansa
Jurnal Penelitian Ilmu Sosial dan Kegamaan Islam
Vol. 20 No. 1 January – June 2023

The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation

Beny Abukhaer Tatara
Asymmetric Warfare Study Program, Faculty of Defense Strategy, The Republic of Indonesia Defense University, Bogor, Indonesia
Email: benyabukhaertatara@gmail.com

Bisma Abdurachman
Asymmetric Warfare Study Program, Faculty of Defense Strategy, The Republic of Indonesia Defense University, Bogor, Indonesia
Email: bismaabdurachman@gmail.com

Desta Lesmana Mustofa
Asymmetric Warfare Study Program, Faculty of Defense Strategy, The Republic of Indonesia Defense University, Bogor, Indonesia
Email: lesmanadesta@gmail.com

David Yacobus
Asymmetric Warfare Study Program, Faculty of Defense Strategy, The Republic of Indonesia Defense University, Bogor, Indonesia
Email: nenimaotriirekiit@gmail.com

Article History
Submitted: November 21, 2022
Revised: February 22, 2023
Accepted: February 24, 2023

How to Cite:
Tatara, Beny Abukhaer, Bisma Abdurachman, Desta Lesmana Mustofa, and David Yacobus. "The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation." *NUANSA: Jurnal Penelitian Ilmu Sosial Dan Keagamaan Islam* 20, no. 1 (2023): 19–37.

http://ejournal.iainmadura.ac.id/index.php/nuansa
DOI: 10.19105/nuansa.v20i1.7362
Page: 19-37

Abstrak:

In the era of the industrial revolution 4.0, many activities use the internet and computers, including economic activities. Many activities in real space are transformed into cyberspace. Currently, the world economy is transforming from conventional methods to digital. Thus, almost all countries in the world are competing to adapt to these changes, one of which is Indonesia which, based on the McKinsey report, ranks first as the country with the fastest growth in adopting the digital economy. The purpose of writing this article is to analyze the potential for cyber attacks that can affect the transformation of Indonesia's digital economy. The research method used is qualitative with data collection techniques in the form of literature studies. The results of the study found that there are several potential cyber attacks in the transformation of Indonesia's digital economy, including: Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Man-in-the-middle (MitM) attacks, Phishing attacks, Drive-by-download attack, Password Attack, SQL Injection Attack, Cross-site scripting (XSS) attack, Eavesdropping attack, Birthday Attack, and Malware Attack.

(Pada era revolusi industri 4.0, banyak aktivitas yang menggunakan internet dan komputer, termasuk aktivitas ekonomi. Banyak aktivitas di dunia nyata ditransformasikan ke dunia maya. Saat ini, perekonomian dunia sedang berubah dari metode konvensional ke digital. Oleh karena itu, hampir semua negara di dunia sedang bersaing untuk menyesuaikan diri dengan perubahan ini, salah satunya adalah Indonesia yang, berdasarkan laporan McKinsey, menduduki peringkat pertama sebagai negara dengan pertumbuhan tercepat dalam mengadopsi ekonomi digital. Tujuan penulisan artikel ini adalah untuk menganalisis potensi serangan cyber yang dapat mempengaruhi transformasi ekonomi digital Indonesia. Metode penelitian yang digunakan adalah kualitatif dengan teknik pengumpulan data berupa studi pustaka. Hasil penelitian menemukan bahwa ada beberapa potensi serangan cyber dalam transformasi ekonomi digital Indonesia, di antaranya: Serangan Denial-of-service (DoS) dan distributed denial-of-service (DDoS), Serangan Man-in-the-middle (MitM), Serangan Phishing, Serangan Drive-by-download, Serangan Password, Serangan SQL Injection, Serangan Cross-site scripting (XSS), Serangan Eavesdropping, Serangan Birthday, dan Serangan Malware.)

Kata Kunci:

Cyber Attack; Digital Economy; Transformation; Indonesia

Introduction

Rapid developments in information technology have given the global population a new era, namely the industrial revolution 4.0 era which is marked by the development of various technological innovations, such as the Internet of Things (IoT), Cloud Computing, and Artificial Intelligence (AI). Developments and innovations in information technology have changed many aspects of human life, from lifestyle, work, to economic activities. Advances in technology have enabled the emergence of several digital-based business models, which are significantly more efficient and innovative, bringing with them both opportunities and challenges that require proper management.

The industrial revolution 4.0 is all about digital transformation[1]. With the digitalization movement, people can now carry out economic activities regardless of space and time. Economic transactions can be done anywhere, anytime, and from anywhere. Companies need to change and meet the needs that arise as a result of digital transformation in the economy for their business continuity, considering that in the business world, digital transformation has become a necessity that cannot be ignored. All industry players have taken initial steps towards it. The Corona Viruse Disease 2019 (COVID-19) pandemic also has accelerated digitalization processes, as more and more people have continued, to the extent possible, with their activities through online channels for example, for working, studying, communicating, selling and buying, or entertainment[2].

In Indonesia, along with the growth and development of the increasing population, internet users are also experiencing a growth rate. According to data from the Ministry of Communications and Information Technology, the number of Indonesian internet users in 2021 increased 11 percent from the previous year, from 175.4 million to 202.6 million users[3]. This also has an impact on the increasing growth of strategic and widespread use of digital technology, including social media and e-commerce. The rapid growth of digital in recent years indicates that the process towards digital transformation in Indonesia has become increasingly massive. So that the government is committed to encouraging digital transformation by accelerating the development of digital infrastructure, including high-speed internet and digital capabilities with the collaboration of the government, the public and the private sector to be able to invest in digital technology such as cloud, data center, security management and broadband infrastructure. Indonesia will also harmonize digital standards, in accordance with global norms, to encourage collaboration between industry players so that they can accelerate digital transformation, including the digital transformation of the economy[4].

Digital economy is defined as economy base on electronics goods and services and formed by electronic business models, integrated with global network of economy and social, enabled by ICT such as internet technologies[5]. This includes activities such as buying and selling, banking, and accessing education or entertainment using the Internet or connected devices. So, the growth and potential of digital economy depend on the trust on

---

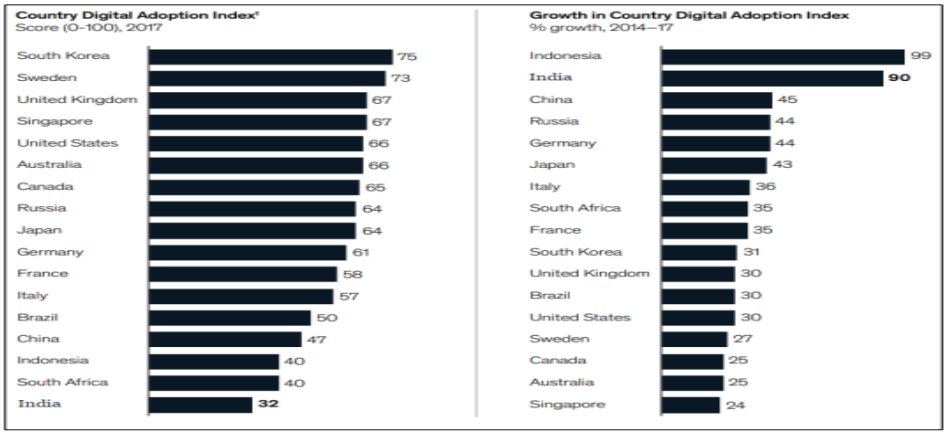
[1] Indonesia Financial Services Authority, "Blue Print for Digital Transformation in Banking" (Jakarta, 2021).
[2] United Nations Conference on Trade and Development, *Digital Economy Report 2021* (New York: United Nations Publications, 2021).
[3] Ken Devina, Mai Hendar Santoso, and Rifki Pratama, "The Strategy of Teaching of Preventing Violence in Cyber Media by Journalism Lecturer of UIN Syarif," *Jurnal Huriah : Jurnal Pendidikan Dan Pnelitian* 2, no. 4 (2021): 78–85.
[4] Indonesian Ministry of Industry, "Indonesia's Fourth Industrial Revolution Making Indonesia" (Jakarta, 2018).
[5] Chooi Shi Teoh and Ahmad Kamil Mahmood, "National Cyber Security Strategies for Digital Economy," *Journal of Theoritical and Applied Information Technology* 95, no. 23 (2017): 6510–22.

the internet and in cyberspace. Cyberspace can be defined as the space in which information circulates from one medium to another and where it is processed, duplicated, and stored. It is also the space in which tools communicate, where information technology becomes ubiquitous[6].

The digital economy substantially drives economic growth[7]. Based on the McKinsey Report, the Indonesian economy is experiencing rapid growth, Indonesia is ranked first as the country with the fastest growth in adopting the digital economy[8]. This is seen from individual, business, and government applications through three pillars. The main assessment is assessed from availability and download speed, digital reach of data consumption per user, and digital value of use in digital payments or e-commerce. Indonesia's score is 99 percent, followed by India 90 percent, China 45 percent, and Russia 44 percent. In fact, it is claimed that the digital economy will become Indonesia's opportunity in 2025. Digitization in Indonesia includes the Manufacturing Sector with US$ 34 billion, the Retail Sector with US$ 24.5 billion, the Transportation Sector with US$ 15.5 billion, the Mining Sector with US$ 14.8 billion, and the Mining Sector with US$ 14.8 billion. Agriculture is US$ 11 billion, Media Sector is US$ 7.9 billion, Health Sector is US$ 6.6 billion, Public Sector is US$ 4.8 billion, and the Financial Sector is US$ 1.8 billion.

Figure 1

Growth in Country Digital Adoption Index % growth, 2014–2017[9]



The rapid development of Indonesia's digital economy has had a major impact on increasing the national economy. But on the other hand, the increase in the digital

[6] Thomas A Johnson, *Cybersecurity : Protecying Critical Infrastructures from Cyber Attack and Cyber Warfare* (London: CRC Press, 2015).

[7] Australia Indonesia Partnership for Economic Governance, *The Digital Economy in Indonesia* (Jakarta: Indonesia Competition Commissin, 2017).

[8] McKinsey Global Institue, "Digital India : Technology to Transform a Connected Nation," 2019.

[9] McKinsey Global Institue, 2019

economy in Indonesia also poses risks that need to be anticipated. According to Abdul Rahim [10], that the digital economy is faced with the real risk of threats and vulnerabilities of cyber attacks and cybercrimes where hackers and cybercriminals are involved in an attempt to infiltrate critical government and private business information for internet fraud. On this basis, this paper would like to review related to the potential cyber attacks in Indonesia's digital economy transformation.

Research Method

This study uses a qualitative method with a descriptive approach. Related to the approach used in this study, Kenneth D. Bailey defines descriptive research is a research that aims to provide an overview of a phenomenon in detail (to describe what happened)[11]. The data collection technique used is form a literature study. According to Creswell[12], a literature study is research conducted by examining qualitative documents such as books, journals, newspapers, magazines, reports, and other documents relevant to the research. Based on the foregoing, the data collection in the research. This is done by reviewing and / or exploring several journals, books, and documents (either in the form of print or electronic) as well as other sources of data and/or information considered relevant to the research or study. The data analysis technique used in this study consists of three steps, namely data collection, data presentation, and concluding/verification[13].

Results and Discussion

Cyber Attacks

In the Talinn Manual on the International Law Applicable to Cyber Warfare, cyber attack is defined as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects[14]. Cyberattack is a kind of attack that targets computer or computer network in an attempt to steal, alter or destroy any critical data present in it[15]. Cyber-attack can be operated either by an individual or by groups. The aim of cyber-attack is to get the information system of an

---

[10] Bakri Mat et al., "Cybersecurity and Digital Economy in Malaysia : Trusted Law for Customer and Enterprise Protection," *International Journal of Innovative Technology an Exploring Ebgineering (IJITEE)* 8, no. 8S3 (2019): 214–20.

[11] Kenneth D. Bailey, *Methods of Social Research*, 4th ed. (Ney York: The Free Press, 2007).

[12] John W Creswell and Cheryl N Poth, *Qualitative Inquiry & Research Design; Choosing among Five Approach*, 3rd ed. (California: Sage Publications, Inc, 2018).

[13] M.B. Miles, A.M. Huberman, and J. Saldana, *Qualitative Data Analysis : A Methods Sourcebook*, 3rd ed. (California: Sage Publications, Inc, 2014).

[14] Michael N Schmitt, *Talinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N Schmitt (New York: Cambridge University Press, 2013).

[15] Jibi Mariam Biju, Neethu Gopal, and Anju J Prakash, "Cyber Attacks and Its Different Types," *International Research Journal of Engineering and Technology (IRJET)*, 2019, 4849–52.

individual or a management. Cyberattack make use of malicious code and hence it changes the computer data, code or logic. The first generation of cyber attacks occurred in the 1980s. Currently, cyber attacks are entering their fifth generation. The description of cyber attack generation is in the table below:

Table 1
Generation af Cyber Attacks[16]

Generation	Overview	Examples of known incident
Gen. 1	The first generation began in the 1980s and coincided with the mass availability and use of personal computers by the general public. Virus attacks, which are malicious software programs that replicate themselves on new computers, soon emerged. These virus attacks affected all businesses and users of personal computers. The impact of virus attacks was large and disruptive enough that commercial anti-virus software products were developed to protect against them.	1.Elk Cloner Elk Cloner is known as the first virus written and released to infect personal computers. Coded by then 15-year old Richard Skrenta as a joke, it served as an annoyance and occasionally displayed a poem on the infected computer. 2.Brain Brain is known as the first worldwide virus. It was created in 1986 by mistake when two brothers, Basit and Amjad Farooq Alvi wrote what they thought was a mechanism to halt illegal copying of their software products. However, their design was flawed and their tool became an actual virus that copied and replicated itself.
Gen. 2	The second generation emerged in the 1990s with the advent of networking and the internet. Everyone was "going online." With networks connecting computers and the internet connecting governments, businesses and the public, the gates were opened for the broad and rapid spread of malicious and volatile software. This unencumbered access to	1.Moris Worm The Morris worm was launched in the very early days of the Internet, on November 1988. Robert Morris, a graduate student at Cornell University, created the Morris Worm with innocent intentions. He claims he wrote the worm in an effort to gauge the size of the Internet. Unfortunately, the worm contained an error that caused it to repeatedly infect computers which consumed resources creating a denial of service conditions. The Morris Worm is said to have infected as many as 60,000 host systems across the young Internet and served notice that network and Internet security was

[16] Check Point Software Technologies, *5th Generation Cyber Attacks Are Here and Most Businesses Are Behind : A New Model for Assessing and Planning Security* (Tel Aviv: Check Point Software Technologies Ltd, 2018).

	anything and everything connected, led to the development of the network firewall.	severely needed. 2.Melissa Virus In 1999, David Smith, a network programmer, released the Melissa Virus to the Internet. It was contained in a Microsoft Word document macro that when opened would email itself to the first 50 addresses in the MAPI email address file on the computer. Smith's motivation was apparently curiosity. Melissa crashed 100,000 email servers and caused $80M in damages.
Gen. 3	The third generation emerged in the early 2000s as attackers learned to leverage vulnerabilities in all components of an IT infrastructure. IETF RFC 2828 defines "vulnerability" as "A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy." And vulnerabilities were plentiful. At any given time, multiples of them existed in operating systems, applications—any element of an IT infrastructure had vulnerabilities that an adept attacker could take advantage of to gain access to a private network. Attacks targeting vulnerabilities could not be effectively stopped by firewalls, anti-virus or intrusion detection system (IDS) products. So, IDS products advanced into intrusion prevention systems (IPS) to not only detect but to actually prevent attacks targeting vulnerabilities.	1.ILOVEYOU The ILOVEYOU virus launched on May 4, 2000 and in a matter of minutes infected thousands of computers. It was so far reaching and impactful that it made the cover of Time magazine in May 2000. Companies and anti-virus vendors screened emails with a title of "ILOVEYOU" but attackers simply changed the title to continue its proliferation. 2.SQLSlammer SQLSlammer, aka Sapphire among other names, attacked vulnerabilities in Microsoft SQL Server and MSDE and became the fastest spreading worm of all time 3.Estonia On April 27, 2007, European Union and NATO member country Estonia fell under massive cyber-attacks against its infrastructure.

Gen. 4	The fourth generation emerged in approximately 2010 as attackers reached new levels of sophistication. In fact, attackers and their methods became professional. The attacks ranged from international espionage to massive breaches of personal information to large scale internet disruption. This generation's attacks made headlines in daily, mainstream media simply because of the large scale impact on and relevance to the general public. The attacks impacted board rooms, CEOs and caused governmental investigations. While internet security of the 2nd and 3rd generations provided access control and inspected all traffic, it was severely lacking in validating the actual end-user content received in email, through file downloads and more. Attacks were hidden in everything from resumes to picture files and behind them awaited sophisticated code ready to launch and spread and sometimes was further supported by massive bot armies ready to storm the gates. All that was needed was for a user to do their job—such as opening an attachment in the official looking email in their In-box or download a business file from the internet or plug a USB into their laptop—and the attack was silently	1.Stuxnet Discovered in the Fall of 2010, the Stuxnet worm attacked Iran's Natanz nuclear refinement facility. Described by some as the most advanced attack ever designed, Stuxnet searched for the specific Siemen's controllers that managed the nuclear centrifuges in Iran's facility and once infected, stealthily caused them to spin out of control, ultimately causing physical damage to the centrifuge equipment. It was later reported that Stuxnet was created via a joint effort between the United States and Israel in an effort to impede Iran's nuclear ambitions. 2.DYN On Friday, October 21, 2016, cyber security reached yet a new level of public awareness, as the world learned that an army of bots hosted on internet connected cameras were able to cause outages to well known internet services such as Twitter, Amazon, Spotify and Netflix. The global Distributed Denial of Service (DDoS) attack on DYN, a large DNS infrastructure company, caused the downtime. It may not have shocked internet security professionals, but it gave yet another demonstration of the fragility of the Internet grid. Fortunately, it was not as damaging as it could have been. 3.Target In December 2013, Target, the third largest US retailer reached headlines over a cyber-attack that planted malware on their point of sale (POS) system and compromised upwards of 40 million customer credit and debit cards and the private information of as many as 110 million customers (various reports claim from 70 to 110 million). It was reported that the attackers first breached the network of Target's HVAC provider who had remote access to Target's network for purposes of HVAC service in some Target stores. From there the attackers were able to plant the malware in the Target point of sale (POS) system to capture and export credit card and other personal information before it was encrypted and sent on to Target's

	launched. The attack could search for customer databases and exfiltrate personal information, or via communication back to "Command&Control" (C&C) initiate a massive bot-driven denial of service attack for purposes of disruption or as a decoy for the real attack, and much more.	transaction processing. The financial impacts of the breach were estimated to reach into hundreds of millions of dollars with some estimates as high as $1B. In addition,Target's CEO and Board Chairman Gregg Steinhafel resigned.
Gen. 5	The 5th generation emerged in approximately 2017 as leakage of advanced tools drove large scale, multi-vector, mega attacks that generated revenues and disruption for the criminals and caused major impacts on a large scale. This led to custom, sophisticated malware that can infiltrate and proliferate from and to virtually any vector of an IT infrastructure—including a business's networks, cloud instances, remote offices, mobile devices, third parties and more. This latest, 5th generation of attacks is well described in The Global Risks Report 2018, 13th Edition, "incidents that would once have been considered extraordinary are becoming more and more commonplace." And the report later cites two attack examples during 2017 saying, "the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses	1.WannaCry In May 2017 the WannaCry ransomware attack hit and targeted computers running the Microsoft Windows XP operating system worldwide. The attack encrypted data and then demanded a ransom payment to be made in Bitcoin. WannaCry leveraged a tool called EternalBlue that was developed by the United States National Security Agency—and was presumably unintentionally leaked to the cyber world. 2.NotPetya In March 2016 Petya ransomware appeared. It encrypted hard drives and demanded a ransom in exchange for the key to decrypt the files. Then in June 2017 an attack initially thought to also be Petya attacked banks, airports and power companies in Ukraine, Russia and parts of Europe. After deeper analysis it was dubbed NotPetya because it truly was not The Petya attack encrypted files and actually offered a process to pay ransom to attain the decryption key to free the files. NotPetya also encrypts files but only appears to offer a means to buy the decryption key. The token on its ransom screen is merely a randomly generated number that is meaningless. However, among the most impacted by the attack is one of the largest shipping companies in the world, A.P. Moller-Maersk. Based in Copenhagen, the attack caused shipping delays and disruption for weeks and an estimated financial impact of between $200-$300 million

	of US$300 million for a number of affected businesses."

Various types of cyber attacks today are as follows [17]: First, Denial-of-service (DoS) and distributed denialof-service (DDoS) attacks. A denial-of-service attack overruns the system resources so that it cannot answer to the service request. The host machine which are affected by malicious software that are controlled by an attacker launches DDoS attack. In this kind of cyber-attack, the machine or network resources are made unavailable for the intended user by disturbing the service of the host which is connected to the internet. It is very difficult to prevent DoS attack as it is very challenging to differentiate a legitimate one from a malicious traffic request as they use same port and protocol. In order to protect the system from denial-of-service attack, make sure that the system contain IDS, DDoS protection product. It is necessary to ensure that there is surplus of bandwidth internet connection on a particular organization. As there is large bandwidth for service traffic requests, it helps to protect against low-scale DDoS attacks.

Second, Man-in-the-middle (MitM) attack. A MitM attack takes place when a third party comes in between the communication of a client and a server. The third party impersonates both the client and the server and gain access to the information between them. This kind of attack makes a threat actor to seize, sent and receive the data which intended for someone else others. A MITM attack misuses the real time operation of transactions, communication or exchange of other information. The different types of man-in-the-middle attack includes session hijacking, IP spoofing and reply. An intrusion detection system can be set up in order to avoid man-in-middle attack. It helps to give immediate alert if someone tries to hijack the network flow. Virtual private network can also be used to prevent man-in-middle attack. This helps to create additional secure layers when accessing a company's confidential layer via Wi-Fi.

Third, Phishing attacks. Phishing attack is the means of sending fraudulent emails that seems to come from trusted sources. The main goal of this kind of attack is gaining personal and credential information. Phishing attack is a form of social engineering and technical trickery. It is in the form of emails which consists of embedded hyperlinks that loads malware onto our system. Sometimes this link also leads to an illegitimate website that makes us to download malware or give up our personal information. To get sensitive data phishing attack make use of some media tools, messages, calls etc. whaling, spear

[17] Muhamad Rizal and Yanyan M Yani, "Cybersecurity Policy and Its Implementation in Indonesia," *Journal of ASEAN Studies* 4, no. 1 (2016): 61–78; Andreea Bendovschi, "Cyber-Attacks – Trends , Patterns and Security Countermeasures," *Procedia Economics and Finance* 5671, no. December 2015 (2016), https://doi.org/10.1016/S2212-5671(15)01077-1; Biju, Gopal, and Prakash, "Cyber Attacks and Its Different Types."

phishing, pharming and deceptive are the different phishing techniques. In order to reduce the risk of phishing attack, critical thinking, hovering over the links, analyzing email headers and sandboxing can be used. Moreover, by giving awareness among the organization employees as well as for individuals we can prevent phishing attack to some extent.

Fourth, Drive-by- download attack. Drive-by-download attack is a common kind of cyber-attack carried out by the cyber criminals to spread malware and gain unauthorized access. This attack occurs when a computer becomes infected by a malicious software by simply visiting a website. The user does not need to click anywhere to get infected, that's why it is called" drive-by" download attack. Here the criminals often use a legitimate website and inject a malicious object inside the web pages. The users cannot observe the infections and range from malicious JavaScript code to iFrames, links, redirects, crosssite scripting, and other malicious elements. At the time when a user visits that infected web page, malicious codes are automatically loaded into the user's browser. Then it suddenly scans the computer security vulnerabilities in the operating system and other applications. Updating the software quickly and regularly, removal of unwanted software applications and browser plug-in, by using firewall and web filtering software can be used to prevent drive-by download attack. Moreover, any kind of malicious software can enter itself into a system without any explicit permission when we are using a privileged account whenever to browse the internet. Such entry to the system can be prevented by keeping two separate account. One can be used for daily activities and other can be used for administrator account for installing software.

Fifth, Password Attack. The most common method to authenticate user is to use passwords and obtaining such passwords is an effective attack approach. Password attack is the technique in which user's password is obtained or decrypted by illegitimate means. User password can be obtained by looking around the user's desk, by guessing, accessing password database, sniffing the network connection to get the plaintext password etc. Password sniffers, dictionary attacks, cracking programs are the different methods used by the cyber criminals in password attack. By changing the passwords frequently, using unrecognizable words and minimum length can the different means by which password attack can be defended. Brute force and dictionary attack are the two main techniques in which password can be obtained. Brute force is a random method in which different passwords are tried expecting that one password will word whereas the later method gain access to a user's computer and network.

Sixth, SQL Injection Attack. SQL (Structured Query Language) is a computer language that is used to store, manipulate and retrieve data stored in the database. SQL language uses commands like select, update, delete to perform the required task. SQL can also execute queries against the database, insert records to the database and can create new

tables in the database. SQL Injection (SQI) attack make use of malicious code in order to access information by manipulating database at the backend. This information may include any sensitive organization details, customer/ user private data etc. This may result in the illegal viewing of the user data, deletion of the table data and unauthorized attack of database. An attacker who wants to execute SQL injection will manipulate a standard SQL query to exploit vulnerabilities in a database that are not validated. Attackers can also use misfiltered characters to alter SQL commands. There are several effective ways to prevent and protect against SQLI attacks if they occur. Input validation can be performed to identify unlawful user inputs which is the writing code practice that can. But this method is not much suitable as the mapping of all legal and illegal inputs is not feasible. Because of this, usually a web application firewall (WAF) is used to remove out SQLI. Signature recognition, IP reputation and other security methods can also be used to identify and block SQL injections with a minimum of false positives.

Seventh, Cross-site scripting (XSS) attack. Cross-site scripting is a common type of injection attack that inserts malicious code into a trusted web site or into a sensitive web application. In other words, XSS occurs when the attacker injects a malicious code or JavaScript into website's database. The intruder injects malicious JavaScript code into the end user's webpage and make him/her to download the webpage. The browser of the victim executes the malicious script within the response, sending the cookies of the victim to the server of the attacker. There are three main types of XSS attack: Persistent XSS, Reflected XSS and DOM based XSS. In persistent XSS, malicious code arose from the website's database whereas in case of Reflected XSS, malicious code arose from the victim's request. DOM based XSS is an alternate for above mentioned methods. Here the vulnerability is present in the client side not in the server side. Cross-site scripting can be prevented either by encoding or validation. Encoding escapes the user input so that the browser interprets it only as data, not as code and validation filters the user input to be interpreted by the browser as code without malicious commands.

Eighth, Eavesdropping attack. Also known as sniffing or snooping attack. Eavesdropping attack deals hacking data that are sent through digital devices. Attacker uses insecure network for communication and examines send and receive data. As they do not show any abnormal operation during transmission via network, this kind of attack are very hard to detect. Using this method an attacker can obtain various information like credit card number, password and other sensitive information that are sent across the network. Attacker may introduce sniffer on a computer or server to perform the eavesdropping attack seize data during transmission. This attack can be of two types: Passive Eavesdropping and Active Eavesdropping. Passive Eavesdropping takes place by listening to the message transmission in the network, attacker uncovers the data. In Active

Eavesdropping, attacker get the data by pretending himself as a friendly unit and sending transmitter queries. Use of an anti-virus software, firewall, virtual private network, encryption and avoiding the public network for transmitting sensitive data helps to prevent eavesdropping attack.

Nineth, Birthday Attack. Birthday attack is a kind of cryptographic attack belonging to a brute force attack class. It works on the principle of birthday problem in probability theory. This attack can be used to misuse the exchange of information between more than two parties. Birthday attacks are carried out using hash algorithms to check the message integrity, software or digital signature. Hash function processed message produces a message digest of fixed length. This message digest exclusively defines the input message as it is independent of the length of the input message. Birthday attack is the process of finding two arbitrary message that generate same message digest when processed by a hash function. If the sender calculated message digest is same as that of the message digest calculated by an attacker, the attacker can replace the message of sender with attacker message. Thereby the receiver of the message cannot recognize the message as fraud as it shows same message digest.

Tenth, Malware Attack. Malware attack is a class of cyberattack in which malicious software is installed into the user's computer without any consent of the user. This is what we called now as virus, spyware or ransomware etc. Malicious code is attached to the legitimate code, get propagated and executed by themselves. Malwares are able to access private network, interrupt certain computing operation, steal sensitive information or any other user data and thereby making money illicitly from the target. Now a day, malware aims more at business or financial information than any credential personal information. Most common type of malware includes: Virus, a malicious software that get attached to any computer program, replicate and modify codes when executed. It can spread either by downloading a file or running any program. Worms, spread across computers or networks via email attachments. This may result in denial-ofservice attacks. Trojans, one of the most danger malware which has malicious function. It hides in a useful program and do not replicate like viruses. Ransomware, a type of malicious software that locks out the user data and threatens user unless a ransom is paid. It is very difficult to prevent this attack even though the code is simple. Spyware, a kind of malware that inspects the user activity without user approval and report it to the attacker.

Digital Economy

The definition of the digital economy has evolved Since first coined in the mid-1990s along with the fast internet at that time. As Internet use expanded, reports from the mid-2000s onwards focused increasingly on the conditions under which the Internet economy might emerge and grow. It reflects the rapidly changing nature of technology and

its use by enterprises and consumers[18]. Definitions evolved to include analyses of different policies and digital technologies, on the one hand, and the growth of ICT and digitally oriented firms as key actors, on the other[19]. Because it is a world that is only in the early stages of digitization, the thriving digital economy does not have a widely accepted definition. there are many interpretations of the same term in the literature and analysis, as well as in different forms. Part of what makes defining the digital economy difficult is the rapidly changing nature of technology[20]. On the one hand this may be due to the novelty and lack of adequate understanding or clarity of this phenomenon, but on the other hand the time required to agree on a standard definition often lags the pace of technological change. The following summarizes the definitions of the digital economy from various sources :

Table 2
Evolving definitions and concepts of the digital economy[21]

Source	Definition
House of Commons 2016: The Digital Economy	"The digital economy refers to both the digital access of goods and services, and the use of digital technology to help businesses".
G20 DETF 2016: G20 Digital Economy Development and Cooperation Initiative	"...a broad range of economic activities that include using digitized information and knowledge as the key factor of production, modern information networks as an important activity space, and the effective use of information and communication technology (ICT) as an important driver of productivity growth and economic structural optimization".
Elmasry et al. 2016: Digital Middle East: Transforming the Region into a Leading Digital Economy (Digital McKinsey)	No explicit definition: "less as a concept and more as a way of doing things", but with three attributes: "creating value at the new frontiers of the business world, optimizing the processes that execute a vision of customer experiences, and building foundational capabilities that support the entire structure".

[18] Kevin Barefoot et al., "Defining and Measuring the Digital Economy," 2018.
[19] United Nations Conference on Trade and Development, *Digital Economy Report 2019 : Value Creation and Capture Implications for Developing Countries* (New York: United Nations Publication, 2019).
[20] Barefoot et al., "Defining and Measuring the Digital Economy."
[21] Rumana Bukht and Richard Heeks, "Defining, Conceptualising and Measuring the Digital Economy," *International Organisations Research Journal*, no. September (2018), https://doi.org/10.17323/1996-7845-2018-02-07.

Knickrehm et al. 2016: Digital Disruption (Accenture)	"The digital economy is the share of total economic output derived from a number of broad "digital" inputs. These digital inputs include digital skills, digital equipment (hardware, software and communications equipment) and the intermediate digital goods and services used in production. Such broad measures reflect the foundations of the digital economy".
Rouse 2016: Digital Economy	"The digital economy is the worldwide network of economic activities enabled by information and communication technologies (ICT). It can also be defined more simply as an economy based on digital technologies".
Dahlman et al. 2016: Harnessing the Digital Economy for Developing Countries (OECD).	"The digital economy is the amalgamation of several general purpose technologies (GPTs) and the range of economic and social activities carried out by people over the Internet and related technologies. It encompasses the physical infrastructure that digital technologies are based on (broadband lines, routers), the devices that are used for access (computers, smartphones), the applications they power (Google, Salesforce) and the functionality they provide (IoT, data analytics, cloud computing)".
OUP 2017: Digital Economy	"An economy which functions primarily by means of digital technology, especially electronic transactions made using the Internet".

Based on some of the definitions above, it can be concluded that the digital economy is an economic activity that utilizes digital technology in carrying out its economic activities. When digital technology supports more transactions, the digital economy becomes increasingly inseparable from the functioning of the economy as a whole. The different technologies and economic aspects of the digital economy can be broken down into three broad components[22]:

First, Core aspects or foundational aspects of the digital economy, which comprise fundamental innovations (semiconductors, processors), core technologies (computers, telecommunication devices) and enabling infrastructures (Internet and telecoms networks). Second, Digital and information technology (IT) sectors, which produce key products or services that rely on core digital technologies, including digital platforms, mobile applications and payment services. The digital economy is to a high degree affected by innovative services in these sectors, which are making a growing contribution to

[22] United Nations Conference on Trade and Development, *Digital Economy Report 2019 : Value Creation and Capture Implications for Developing Countries*.

economies, as well as enabling potential spillover effects to other sectors. Third, A wider set of digitalizing sectors, which includes those where digital products and services are being increasingly used (e.g. for e-commerce). Even if change is incremental, many sectors of the economy are being digitalized in this way. This includes digitally enabled sectors in which new activities or business models have emerged and are being transformed as a result of digital technologies.

Potential Cyber Attacks in Indonesia's Digital Economy Transformation

Indonesia ranks first as the country with the fastest growth in adopting the digital economy. The digital economy adoption growth index is calculated based on the level of digital application by individuals, businesses, and governments on three pillars. The three pillars are digital foundation (availability and download speed), digital reach (data consumption per user), and digital value (use in digital payments or e-commerce). The score obtained by Indonesia is 99%, followed by India 90%, China 45%, and Russia 44% [23]. This makes Indonesia predicted to grow into a digital economy giant in Southeast Asia by 2025[24]. The growth of Indonesia's digital economy is expected to be the fastest in the Southeast Asia in 2025 with a number reaching around US$133 billion[25]. Even, the Indonesian digital economy has bright future and is predicted to grow up to eightfold by 2030. The growth of the digital economy will reach eightfold from Rp632 trillion to Rp4.531 trillion. E-commerce will play a crucial role with 34 percent growth or equivalent to Rp1,900 trillion, followed by several other sectors, namely B2B (business-to-business) with an increase of thirteen percent or equivalent to Rp763 trillion and health-tech with an increase of eight percent or equivalent to Rp471.6 trillion[26].

The strategic and widespread use of digital technologies, including social media and ecommerce, has the potential to have significant economic impact, including: Creating an additional 3.7 million jobs by 2025; Generating up to 80% higher growth in revenue for small and medium enterprises (SMEs); and Adding an additional 2% per annum in GDP growth by increasing broadband penetration rates and usage of digital technologies by SMEs[27]. The government is committed to encouraging digital transformation by accelerating the development of digital infrastructure, including high-speed internet and

[23] McKinsey Global Institue, "Digital India : Technology to Transform a Connected Nation."
[24] Google, Temasek, and Bain & Company, "E-Conomy SEA 2019 : Swip Up and To The Right Southeast Asia's $100 Billion Internet Economy," 2019.
[25] Karina Rima Melati and Nur Komala Dewi, "Integrated E-Commerce Ecosystem in China and Indonesia ' s Giant Market," *2nd International Media Conference 2019* 423, no. Imc 2019 (2020): 251–69.
[26] Cabinet Secretariat of The Republic of Indonesia, "Trade Minister: Indonesian Digital Economy to Grow Eightfold by 2030," Setkab.go.id, 2021, https://setkab.go.id/en/trade-minister-indonesian-digital-economy-to-grow-eightfold-by-2030/.
[27] Australia Indonesia Partnership for Economic Governance, *The Digital Economy in Indonesia*.

digital capabilities with the collaboration of the government, the public and the private sector to be able to invest in digital technology such as cloud, data center, security management and broadband infrastructure. Indonesia will also harmonize digital standards, in accordance with global norms, to encourage collaboration between industry players so that they can accelerate economic digital transformation[28]

Besides, the government issued five main principles in developing a digital economy designed by the government through affirmative steps[29], namely: First, Every Indonesian citizen has the same opportunity to access digital channels and become a business actor. Second, Every Indonesian citizen has the right to know to utilize digital technology to be used as a medium for economic activity. Third, every action by the government is to minimize job losses in the event of a transition to the digital economy. Fourth, every legal action that occurs must have a clear and definite legal basis to maintain legal stability in economic activities. Fifth, every vision and mission must be lived out transparently and welcome the digital economy internationally. We know that the Indonesian government aims to advance the digital economy for significant people in business and middle-low to middle-class economic players through these five principles. Furthermore, justice in doing digital business can support the Indonesian economy from its foundation so that the Indonesian state's progress can occur.

However, the introduction of digital technologies in the business processes of an enterprise and its transition to functioning in a digital environment carries new risks and threats that are not inherent in traditional (non-digital) processes and are due to new technologies and features of the digital economy[30], one of them is cyber attack. The National Cyber and Crypto Agency (BSSN) revealed that there were 1.6 billion (1,637,937,022) cyber attacks for the period January-December 2021. The majority found included Malware. Although in Indonesia the majority of cyber attacks are in the form of malware, cyber attacks in other forms also do not rule out the possibility. In the world, the OECD notes that cyber attacks in the form of SQL Injection attacks were the top threat when it comes to web application risks[31]. Types of cyber attacks that have the potential to attack Indonesia's digital economy transformation process include: Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Man-in-the-middle (MitM) attacks, Phishing attacks, Drive-by - download attack, Password Attack, SQL Injection Attack,

[28] Indonesian Ministry of Industry, "Indonesia's Fourth Industrial Revolution Making Indonesia."
[29] Michael Putra Hartanto, Stephanie, and Doni Purnama Alamsyah, "The Digital Economy Growth in Indonesia through E-Commerce," *International Conference on Industrial Engineering and Operations Management*, 2021, 1610–15.
[30] Irina Kirishchieva et al., "Risks and Threats to Economic Security in the Digital Economy," *ICEMT* 01028 (2021).
[31] OECD, "A Roadmap Toward A Common Framework For Measuring The Digital Economy" (Saudi Arabia, 2020).

Cross-site scripting (XSS) attack, Eavesdropping attack, Anniversary Attack, Malware Attack.

Conclusions

Indonesia ranks first as the country with the fastest growth in adopting the digital economy. the introduction of digital technologies in the business processes of an enterprise and its transition to functioning in a digital environment carries new risks and threats, one of them is cyber attack. Potential cyber attacks on Indonesia's digital economy transformation include: Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Man-in-the-middle (MitM) attacks, Phishing attacks, Drive-by - download attack, Password Attack, SQL Injection Attack, Cross-site scripting (XSS) attack, Eavesdropping attack, Anniversary Attack, Malware Attack. Attacks can occur anytime and anywhere, so the government is expected not only to prepare infrastructure to support the development of the digital economy, but also to anticipate by mitigating cyber attacks because the impact of cyber attacks is very large.

REFERENCES

Australia Indonesia Partnership for Economic Governance. *The Digital Economy in Indonesia*. Jakarta: Indonesia Competition Commissin, 2017.

Bailey, Kenneth D. *Methods of Social Research*. 4th ed. Ney York: The Free Press, 2007.

Barefoot, Kevin, Dave Curtis, William Jolliff, Jessica R Nicholson, and Robert Omohundro. "Defining and Measuring the Digital Economy," 2018.

Bendovschi, Andreea. "Cyber-Attacks – Trends , Patterns and Security Countermeasures." *Procedia Economics and Finance* 5671, no. December 2015 (2016). https://doi.org/10.1016/S2212-5671(15)01077-1.

Biju, Jibi Mariam, Neethu Gopal, and Anju J Prakash. "Cyber Attacks and Its Different Types." *International Research Journal of Engineering and Technology (IRJET)*, 2019, 4849–52.

Bukht, Rumana, and Richard Heeks. "Defining, Conceptualising and Measuring the Digital Economy." *International Organisations Research Journal*, no. September (2018). https://doi.org/10.17323/1996-7845-2018-02-07.

Cabinet Secretariat of The Republic of Indonesia. "Trade Minister: Indonesian Digital Economy to Grow Eightfold by 2030." Setkab.go.id, 2021. https://setkab.go.id/en/trade-minister-indonesian-digital-economy-to-grow-eightfold-by-2030/.

Check Point Software Technologies. *5th Generation Cyber Attacks Are Here and Most Businesses Are Behind : A New Model for Assessing and Planning Security*. Tel Aviv: Check Point Software Technologies Ltd, 2018.

Creswell, John W, and Cheryl N Poth. *Qualitative Inquiry & Research Design; Choosing among Five Approach*. 3rd ed. California: Sage Publications, Inc, 2018.

Devina, Ken, Mai Hendar Santoso, and Rifki Pratama. "The Strategy of Teaching of Preventing Violence in Cyber Media by Journalism Lecturer of UIN Syarif." *Jurnal Huriah : Jurnal Pendidikan Dan Pnelitian* 2, no. 4 (2021): 78–85.

Google, Temasek, and Bain & Company. "E-Conomy SEA 2019 : Swip Up and To The Right Southeast Asia's $100 Billion Internet Economy," 2019.

Hartanto, Michael Putra, Stephanie, and Doni Purnama Alamsyah. "The Digital Economy Growth in Indonesia through E-Commerce." *International Conference on Industrial Engineering and Operations Management*, 2021, 1610–15.

Indonesia Financial Services Authority. "Blue Print for Digital Transformation in Banking." Jakarta, 2021.

Indonesian Ministry of Industry. "Indonesia's Fourth Industrial Revolution Making Indonesia." Jakarta, 2018.

Johnson, Thomas A. *Cybersecurity : Protecying Critical Infrastructures from Cyber Attack and Cyber Warfare*. London: CRC Press, 2015.

Kirishchieva, Irina, Mikhail Skorev, Oksana Mishchenko, and Tatiana Grafova. "Risks and Threats to Economic Security in the Digital Economy." *ICEMT* 01028 (2021).

Mat, Bakri, Siti Darwinda Mohamed Pero, Ratnaria Wahid, and Babayo Sule. "Cybersecurity and Digital Economy in Malaysia : Trusted Law for Customer and Enterprise Protection." *International Journal of Innovative Technology an Exploring Ebgineering (IJITEE)* 8, no. 8S3 (2019): 214–20.

McKinsey Global Institue. "Digital India : Technology to Transform a Connected Nation," 2019.

Melati, Karina Rima, and Nur Komala Dewi. "Integrated E-Commerce Ecosystem in China and Indonesia ' s Giant Market." *2nd International Media Conference 2019* 423, no. Imc 2019 (2020): 251–69.

Miles, M.B., A.M. Huberman, and J. Saldana. *Qualitative Data Analysis : A Methods Sourcebook*. 3rd ed. California: Sage Publications, Inc, 2014.

OECD. "A Roadmap Toward A Common Framework For Measuring The Digital Economy." Saudi Arabia, 2020.

Rizal, Muhamad, and Yanyan M Yani. "Cybersecurity Policy and Its Implementation in Indonesia." *Journal of ASEAN Studies* 4, no. 1 (2016): 61–78.

Schmitt, Michael N. *Talinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N Schmitt. New York: Cambridge University Press, 2013.

Teoh, Chooi Shi, and Ahmad Kamil Mahmood. "National Cyber Security Strategies for Digital Economy." *Journal of Theoritical and Applied Information Technology* 95, no. 23 (2017): 6510–22.

United Nations Conference on Trade and Development. *Digital Economy Report 2019 : Value Creation and Capture Implications for Developing Countries*. New York: United Nations Publication, 2019.

———. *Digital Economy Report 2021*. New York: United Nations Publications, 2021.