

ACHIEVING THE INDONESIA NATIONAL CYBER STRATEGY'S OBJECTIVES
BY TAILORING INTERAGENCY INTEROPERABILITY

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

ALZAKI, MAJOR, ARMY
M.M. Yogyakarta, Indonesia, 2015
B.A. Bekasi, Indonesia, 2011

Fort Leavenworth, Kansas
2019

Approved for public release; distribution is unlimited. United States Fair Use determination or copyright permission has been obtained for the use of pictures, maps, graphics, and any other works incorporated into the manuscript. This author may be protected by more restrictions in their home countries, in which case further publication or sale of copyrighted images is not permissible.

REPORT DOCUMENTATION PAGE				<i>Form Approved</i> <i>OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 14-06-2019		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) AUG 2018 – JUN 2019	
4. TITLE AND SUBTITLE Achieving the Indonesia National Cyber Strategy's Objectives by Tailoring Interagency Interoperability				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Alzaki				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301				8. PERFORMING ORG REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Three pillars of national activity in cyberspace are the governance, economic, and security which covers national security and national defense. Cyberspace, which mostly links to Information and Communication Technologies (ICTs), has significant roles in leveraging Indonesia national objectives and protecting national interests. However, this virtual world provides enormous threats in national and international levels that could deter those achievements. Those threats cause the three pillars vulnerable before they are effectively sustained and tailored to achieve national objectives. Cyber resilience capacity and capability are the primary requirements to solve those issues enabled by the existing of National Cyber Security Strategy and National Cyber Security Agency. This thesis seeks to gain how these three pillars can be tailored, to achieve a national comprehensive approach by creating an interoperability interagency system, to leverage national cyber resilience capacity and capability.					
15. SUBJECT TERMS ICTs, Cyber Resilience, Interagency, Interoperability, National Cyber Security Strategy, National Crypto and Cyber Agency					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT (U)	18. NUMBER OF PAGES 135	19a. NAME OF RESPONSIBLE PERSON
a. REPORT (U)	b. ABSTRACT (U)	c. THIS PAGE (U)			19b. PHONE NUMBER (include area code)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Alzaki

Thesis Title: Achieving Indonesia National Cyber Resilience Capacity by Tailoring
Interagency Interoperability

Approved by:

_____, Thesis Committee Chair
LTC Michael K. Goodwin, MMAS

_____, Member
Janet G. Valentine, Ph.D.

_____, Member
William T. Pugh, MPA

Accepted this 14th day of June 2019 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

ACHIEVING THE INDONESIA NATIONAL CYBER STRATEGY'S OBJECTIVES
BY TAILORING INTERAGENCY INTEROPERABILITY, by Alzaki, 135 pages.

Three pillars of national activity in cyberspace are the governance, economic, and security which covers national security and national defense. Cyberspace, which mostly links to Information and Communication Technologies (ICTs), has significant roles in leveraging Indonesia national objectives and protecting national interests. However, this virtual world provides enormous threats in national and international levels that could deter those achievements. Those threats cause the three pillars vulnerable before they are effectively sustained and tailored to achieve national objectives. Cyber resilience capacity and capability are the primary requirements to solve those issues enabled by the existing of National Cyber Security Strategy and National Cyber Security Agency. The government is the primary means in achieving the National Cyber Security Strategy's objectives; however, the interoperability interagency is assumed to be the prominent challenge. This thesis seeks to gain how these three pillars can be tailored, to achieve a national comprehensive approach by creating an interoperability interagency system, to leverage national cyber resilience capacity and capability, (page ii)

ACKNOWLEDGMENTS

This effort would not have been permissible without the blessing of the Almighty God. I am especially indebted to my country which provides me with an opportunity to study at Command General Staff College and pursue double master programs. This is the best opportunity to gain new knowledge, build international networking, and know international militaries as well as their cultures. In particular, it gives me opportunity to enroll in MMAS program and accomplish this thesis.

I might not be able to finish this thesis without my committee members' encouragement and guidance. Mr. Pugh intensely reviewed my writing; Dr. Valentine and Dr. Morrison educated me to strategize my thoughts; and, LTC Goodwin, my chair committee member, supported me to finish this product on time. Indeed, I am grateful for guidance from Dr. Baumann, which I am lucky for becoming his student in a small group. I personally thank Mrs. Chaplann, Mrs. Quillin, and especially the Learning Research Center of CGSOC for their kind supports.

The positive and inspiration atmosphere during CGSC allows me to survive; accomplishing MMAS thesis while facing day to day CGSC's large quantity of assignments and school projects. I am grateful of my Team Leader Mr. Bachelor; my Staff Group Adviser LTC. Horgan as the cyber officer; Dr. Valentine my history instructor also my committee member; and Mr. Beasley, my leadership instructor which his teachings contribute some aspects in this thesis. I will also never forget support and care from my sponsors Mr. Stark, Mrs. Hendry, and Major Bowman with their respective families. I personally thank alumni of CGSC whom pay attention to us during this course; COL Triwidodo, COL Santoso, LTC Wenas Inkiriwang, LTC Patria, MAJ Ferdiansyah,

MAJ Amaraldo, MAJ Rusmanto, and so on. I thank all my staff group member: student ambassador MAJ Winistorfer, MAJ Ray also as my neighbor, MAJ Kiser as the chief, and all other twelve warriors. I thank IMS peers from 88 countries all over the world, which needs several pages to mention their name; especially, my countrymates MAJ Paulus, MAJ Delly, and their families.

I am thankful to all of those with whom I have had the pleasure to work during this project and have provided me inspiration and basic knowledge. Each of them provided me with a significant amount of personal and professional guidance and directed me with a remarkable acknowledgment in both scientific research and general culture. They are my teachers and mentors, and they have taught me more than I could ever give them credit for here. They have taught me what a good learner, researcher, and person ought to be.

I owe my National Army for deploying me at the ministry offices. It provides me a rudimentary knowledge about a broad concept of interagency system and, specifically, cyber development. I felt challenges and difficulties in executing some strategic planning because a lack of networking, different level of situational understanding, and different cultures among the agencies. Those experiences provide me a visualization about the urgency of interoperability interagency which drove my thoughts to portray that in this thesis. I was humbly lucky participating in many discussions and international meetings of the establishment of the Indonesia National Cyber Security Agency; a lesson learned beyond my background knowledge.

Nobody has been more important to me in the pursuit of this project than the members of my family. I would like to thank my parents; whose love and guidance are

with me in whatever I pursue. They are the ultimate role models, and they always pray for me. Most importantly, I wish to thank my loving and supportive wife, Mira Amelia, and my two wonderful children, Radinka and Sabiya who provide unending inspiration. They have been recharging my motivation and idea after coming back from CGSC and pursuing another master program. I am proud of them; they are strong and firm. They have been supporting me to accomplish my thesis during weekdays and weekends.

TABLE OF CONTENTS

	Page
MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE	iii
ABSTRACT.....	iv
ACKNOWLEDGMENTS	v
TABLE OF CONTENTS.....	viii
ACRONYMS.....	x
ILLUSTRATIONS	xii
TABLES	xiii
CHAPTER 1 INTRODUCTION	1
Background.....	1
Research Purpose.....	8
Research Questions.....	9
Assumptions.....	9
Definitions	10
Scope.....	14
Limitations	15
Delimitations.....	15
Significance of the Study.....	16
CHAPTER 2 LITERATURE REVIEW	17
CHAPTER 3 RESEARCH METHODOLOGY	31
CHAPTER 4 ANALYSIS	34
Information and Communication Technology’s Role in Indonesia.....	34
ICTs’ Role in Leveraging National Defense and Security	34
ICT’s role in Supporting National Economy	42
Acknowledging Indonesia Economic Development.....	42
Regional and International ICT Development: Indonesian’s Economic Perspective	44
Impact of Cyberspace for the Future Indonesia Economic Development	48
Dilemmas Caused by the Outrages of Cyber Threats and Risks	53
Lessons Learned from International’s Approaches in Achieving Cyber Resilience Capacity	67

The Establishment of Indonesia National Cyber Security Strategy	79
The Indonesia National Crypto and Cyber Agency.....	87
Acknowledging the National Cyber and Crypto Agency	88
Potential Concerns and Solutions for BSSN to Implement the National Cyber Security Strategy	93
Challenges as a New Transform Agency.....	93
Potential Solutions for the Implementation of Government’s Approach in Achieving the National Cyber Security Strategy	96
Leadership Approach: Recognize Risk and Adaptability Capability	97
Leadership Approach: Establishing a Sense of Urgency and Guiding Coalition	98
Organizational Approach: A Networking Model	103
Organizational Approach: Forming a National Operational Guidance or Regulation.....	108
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	112
Conclusions.....	112
Recommendations.....	113
BIBLIOGRAPHY.....	114

ACRONYMS

ACSC	Australian Cyber Security Center
AI	Artificial Intelligence
APJII	<i>Asosiasi Penyelenggara Jasa Internet Indonesia</i> (Indonesian Internet Service Provider Association)
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
BSSN	<i>Badan Siber and Sandi Nasional</i> (National Cyber and Crypto Agency)
CSA	Cyber Security Agency
CSPC	Cyber Security Policy Course
DGDP	Directorate of Graduate Degree Programs
DOS	Disk Operating System
G-20	Group of 20
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
Id-SIRTII/CC	Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center
IoT	Internet of Things
IT	Information Technology
ITU	International Telecommunication Union
MRI	Magnetic Resonance Imaging
NCSS	National Cyber Security Strategy
OECD	Organization for Economic Co-Operation and Development

OIC	Organization of Islamic Cooperation
ROI	Return of Investment
SGA	Small Group Advisor
SMEs	Small to Medium Enterprises.
UNIDIR	United Nations Institute for Disarmament Research
WCIS	World Cellular Information Service

ILLUSTRATIONS

	Page
Figure 1. Indonesia - the Seventh Largest Internet Users on Earth.....	5
Figure 2. Key Barrier in Adopting the Industrial Internet.....	22
Figure 3. Indonesia National Cyber Security Strategy Framework	27
Figure 4. Research Methodology Portrayal.....	32
Figure 5. Indonesia Economic Growth (1990-2016)	44
Figure 6. Revolution Industry and Evolutionary Aspect of the Society 5.0	47
Figure 7. The Digital Revolution Has Arrived in Indonesia	50
Figure 8. Smartphone Penetration Rate as Share of the Population in Indonesia (2015-2022)	52
Figure 9. Cyber Risk and Responses Framework	54
Figure 10. Cyber Threat Diagram	59
Figure 11. Asia Pacific 2016 Malware Infection Index	66
Figure 12. Key Barrier in Adopting the Industrial Internet.....	70
Figure 13. Indonesia GCI 2017 Indicator Assessments	72
Figure 14. U.S. Cyber Coordination and Cooperation Model.....	77
Figure 15. National Cyber Security Strategy Framework.....	80
Figure 16. Most Problematic Factors for Doing Businesses	84
Figure 17. An Analysis of Comprehensive Approach of Cyber Networking Model Indonesia Interagency	106

TABLES

	Page
Table 1. Countries Index Cyber Assessment	24
Table 2. Cyber Assessment Indicators.....	25
Table 3. Government's Roles	28
Table 4. Government Development Program	28
Table 5. Two Most Committed Countries Based on GCI 2017 and Indonesia Position ..	74
Table 6. The Most Matured Countries Based on Cyber Maturity in the Asia-Pacific Region 2017, Singapore and Indonesia Position	75
Table 7. Government's Roles	101
Table 8. Government Development Program	102

CHAPTER 1

INTRODUCTION

Background

As the largest archipelagic nation in the world, Indonesia, located between two oceans and two continents has a unique geographical position. This strategic position requires Indonesia to strategize its position carefully. This unique position places Indonesia centrally amongst its ten neighboring countries sea and land borders. Indonesia's territorial seas are essential for Indonesia's international trade. This condition results in Indonesia being vulnerable to security threats. As an archipelago and maritime country, Indonesia is very interested in creating security in the region, including maritime security in order to support Indonesia's interests as the Global Maritime Fulcrum (GMF). Therefore, Indonesia's management of natural resources, its border region, and defense is required.

—Ryamizard Ryachudu, *Defense White Paper 2015*

Three pillars of national activity in cyberspace are the governance, economic, and security which covers national security and national defense. Cyberspace, which mostly links to Information and Communication Technologies (ICTs), has significant roles in leveraging Indonesia national objectives and protecting national interests. However, this virtual world provides enormous threats in national and international levels that could deter those achievements. Those threats cause the three pillars vulnerable before they are effectively sustained and tailored to achieve national objectives. Cyber resilience capacity and capability are the primary requirements to solve those issues enabled by the existing of National Cyber Security Strategy and National Cyber Security Agency. The government is the primary means in achieving the National Cyber Security Strategy's objectives; however, the interoperability interagency is assumed to be the prominent challenge. This thesis seeks to gain how these three pillars can be tailored, to achieve a

national comprehensive approach by creating an interoperability interagency system, to leverage national cyber resilience capacity and capability.

The Indonesia government runs national administration based on national objectives and national interest. Both national elements have been identified since 1945 during the preparation for national declaration for independence. The four pillars of Indonesia national objectives are to protect the Indonesian people and homeland security; promote Indonesian prosperity; educate Indonesian people; and participate in implementing world order based on freedom, peace, and social justice.¹ This thesis focuses on two pillars: protecting the Indonesian people and homeland security and promoting Indonesian prosperity which are identified as the two of three key pillar and consideration in developing a national cybersecurity. The security and economic aspects of deliberation lead to the establishments of national policies that categorize decisive priority actions to protect more than 260 million Indonesians² and build the largest archipelagic country with more than 54,716 Km of coastline³ spreading on the 4,100 Km

¹ Komite Nasional Indonesia Pusat (KNIP), *The Preamble of the Constitution of the Republic of Indonesia 1945* (Jakarta: KNIP, 29 August 1945).

² U.S. Census Bureau, "U.S. and World Population Clock," 14 December 2018, accessed 13 December 2018, <https://www.census.gov/popclock/>; Tumouto, "Jumlah Penduduk Indonesia Tahun 2018 (BPS Prediction)," *Tumoto News*, 5 October 2018, accessed 6 November 2018, <https://tumoutounews.com/2018/05/10/jumlah-penduduk-indonesia-tahun-2018>.

³ California Environmental Associates, *Trends in Marine Resources and Fisheries Management in Indonesia: A 2018 Review*, accessed 9 February 2019, <https://www.packard.org/wp-content/uploads/2018/08/Indonesia-Marine-Full-Report-08.07.2018.pdf>.

line across the equator. Some of its 17,504 islands are the home of 714 ethnicities who speak 600 different languages, along with extensive forest and marine biodiversity.⁴

In economic aspect, Indonesia focuses on economic growth enhancement sustained by a supportive and stabilized environment. Indonesia's position, between the Pacific Ocean and the Indian Ocean, plays a significant role in International trading routes between west and east as a significant strategic sea lane of world oil and trade flow. Indonesia is considered as one of six Middle Power⁵ and is affluent of natural and human resources that are prerequisites for the development of national infrastructure to sustain national growth. For decades, Indonesian leaders have shown great interest in a digital economy to increase the prosperity of their nation and Indonesian people.⁶ The current administration schemes a path for Indonesia to become the greatest digital economy in the Southeast Asia region by 2020.⁷ Also, in order to support the vision of

⁴ Eko Prasetya, "Dari 17.504 Pulau di Indonesia, 16.056 Telah Diverifikasi PBB," *Merdeka*, 19 August 2017, accessed 6 November 2018, <https://www.merdeka.com/peristiwa/dari-17504-pulau-di-indonesia-16056-telah-diverifikasi-pbb.html>.

⁵ Enrico Fels, *Shifting Power in Asia-Pacific? –2017: The Rise of China, Sino-US Competition and Regional Middle Power Allegiance* (New York: Springer, 2017), 697-698.

⁶ Simon Tisdall, "Joko Widodo Takes Office With Plans For Economic Growth and Political Clout," *The Guardian*, 20 October 2014, accessed 6 November 2018, <https://www.theguardian.com/australia-news/2014/oct/20/joko-widodo-takes-office-in-indonesia>.

⁷ Jet Damazo Santos, "The Big Picture: Indonesia's Partnership with U.S. Investors," US Chamber, November 2017, accessed 6 November 2018, https://www.uschamber.com/sites/default/files/11.2017_investment_report_the_big_picture.pdf.

making Indonesia “the digital energy of Asia,” the government, through the Ministry of Communication and Information, launched startups for the digital economy.⁸ Indonesia has redesigned its economy toward high-value industry supported by the Information and Communication Technologies (ICTs) industry, to include Mobile Internet, Cloud technology, Internet of Things (IoT), Big data, and advanced analytics.⁹ Figure 1 illustrates the significant number of Indonesia internet users which portrays a significant of cyberspace role in influencing national economy.

In security aspect, Indonesia seeks to observe the double-edged of cyberspace consequences. The thriving of the digital economy comes with cyber risks and threats for this large nation, Indonesia. Those threats derive from various types of interests, executed by diverse types of actors to achieve various purposes. Regardless of the types of sources and effects, the enhancement of startups and productivity in the digital economic industry is followed by the increasing apprehension among technology professionals and scholars. These individuals have noticed and identified essential factors regarding privacy, security, conflict, and crime that can occur in cyberspace: hacking, cracking, defacing, sniffing, carding, phishing, scamming, and other illegal activities. Surprisingly, these factors are increasing at a faster rate than people can comprehend.

⁸ Ervina Anggraini, “Indonesia’s Vision: 1,000 Startups By 2020,” *Digital News Asia*, 27 November 2015, accessed 6 November 2018.
<https://www.digitalnewsasia.com/indonesias-vision-1000-startups-2020>.

⁹ Kaushik Das, Michael Gryseels, Priyanka Sudhir, and Khoon Tee Tan, “Unlocking Indonesia’s Digital Opportunity,” McKinsey & Company, October 2016, accessed 8 November 2016,
https://www.mckinsey.com/media/McKinsey/Locations/Asia/Indonesia/OurInsights/UnlockingIndonesias20digital20opportunity/Unlocking_Indonesias_digital_opportunity.ashx.

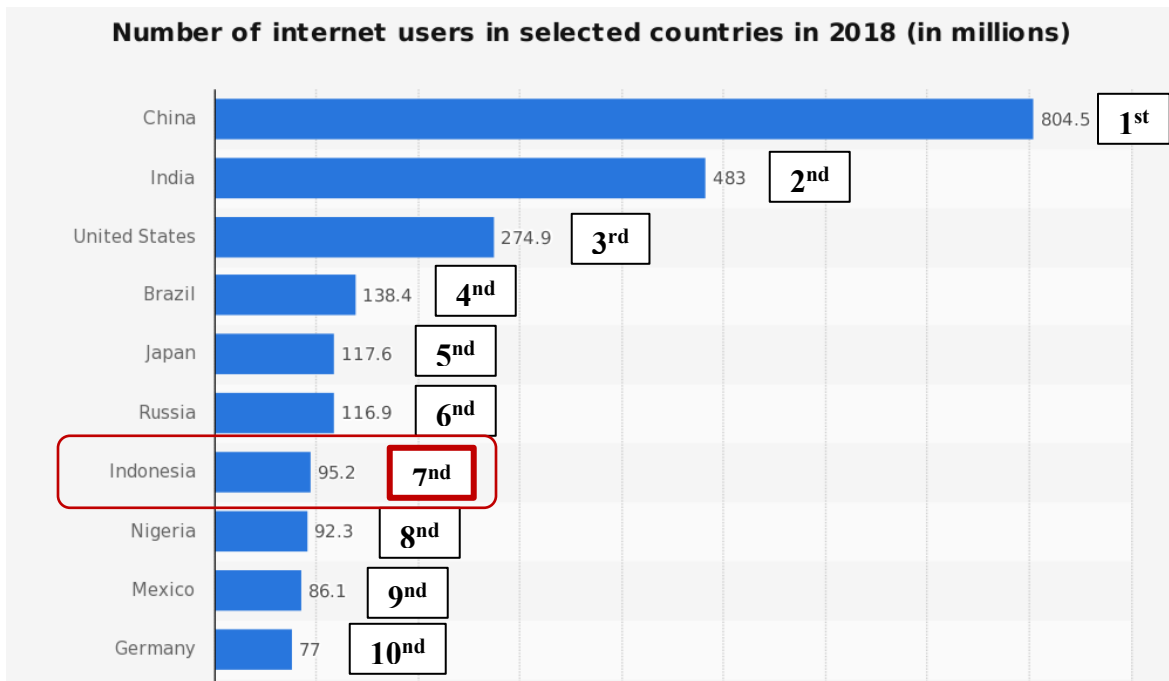


Figure 1. Indonesia - the Seventh Largest Internet Users on Earth

Source: Statista, “Number of Internet Users Worldwide 2018, By Country,” 2019, <https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries/Statistica>.

To integrate those elements, in June 2017, Indonesia proclaimed having the National Cyber Security Strategy as the primary line for achieving national cyber resilience capacity and capability. Its strategic vision is to establish and sustain national cybersecurity capability by synergizing various stakeholders in national security and economic.¹⁰ To achieve the strategic vision, this national strategy has been drafted into

¹⁰ Badan Siber dan Sandi Negara (BSSN), “Remarks the Chief of BSSN about Indonesian National Cyber Security Strategy,” 2018, accessed 31 December 2018. <https://bssn.go.id/strategi-keamanan-siber-nasional/>.

five primary principles: sovereignty, independence, security, togetherness, and adaptive.¹¹ Moreover, this strategy has identified the national cyberspace endstates encompassing cyber resilience capacity in public service security, cyber law enforcement, cybersecurity culture, and digital economy cybersecurity systems. Furthermore, this National Cyber Security Strategy has categorized four key players to succeed executing this strategy consisting of the government, cyber industries, scholars, and cyber communities which are known as “the quad helix.”

The primary key player to succeed the National Cyber Security Strategy is the government. As the center of government cyber efforts, the Indonesia government has established a National Cyber and Crypto Agency namely *Badan Siber and Sandi Nasional* (BSSN). This government agency is projected to enable a strategic environment and promote interoperability, feasibility, acceptability, and trustworthiness of national electronic systems in the success of the National Cyber Security Strategy’s achievements.¹² It has been discussed that cyberspace capability has been used primarily to enhance economic growth, innovation, and efficiency by leveraging digital economic growth with cyber competitiveness and innovation.¹³ Moreover, the major consideration

¹¹ BSSN, “Remarks the Chief of BSSN about Indonesian National Cyber Security Strategy.”

¹² Ibid.

¹³ Rachmatunnisa, “3 Tahun Jokowi-JK, Geber Ekonomi Digital Terinspirasi Silicon Valley,” Inet.Detik, 20 October 2017, accessed 6 November 2018, <https://inet.detik.com/cyberlife/d-3692537/3-tahun-jokowi-jk-geber-ekonomi-digital-terinspirasi-silicon-valley>.

is how to enable the existing agencies, which are supported by cyberspace or ICTs, can work together in a robust and effective system.

The establishment of BSSN adheres to the strategic vision of the National Cyber Security Strategy. It is built to achieve a national cyber security awareness and cyber resilience capacity, and to integrate national all efforts in cyberspace. Therefore, interagency interoperability or cooperation is the fundamental aspect of achieving a robust national cybers resilience capacity and capability. Interagency cooperation is the primary aspect of handling the intertwines of personal, group, national, regional, and international levels of cyber menaces by developing comprehensive efforts to enable the achievement of the National Cyber Security Strategy goals. It will open and simultaneously enhance cyber collaboration, cooperation, and awareness, adapted to a rapidly changing environment that creates a better visualization for cyber resilience growth in both capacity and capability.

However, efforts for tailoring Indonesia's interagency cooperation might be associated with challenges. There are some difficulties to integrate all key pillars of national cyber activities which consist of governance, security, and economic. The primary problem is how to leverage national cyber security strategy achievement by promoting the government's roles consisting of protecting the national cyber environment, national e-Commerce, national critical information infrastructure, and control penetration in regard of ideology, politic, social, cultures, and national defense and security by integrating and synchronizing all exertions to achieve national cyber unity of effort system. While conducting framework arrangements of elements within the new agency of BSSN, formed by three agencies, BSSN is also required to possess a

networking cooperation model with other agencies to conversely provide substantive support in cybersecurity matters throughout national, regional and international scope. This aspect is not less challenging than its role in increasing its capacity building within its new institution. At the last chapter, this thesis provides some possible solution that can address that issue. First, it observes a leadership approach by highlighting a leadership value in comprehending risks and creating adaptability of the agencies. This aspect also discusses about how significant the existence of a sense of urgency and guiding the coalition of organizations in shaping a climate and culture of organization toward the achievement of interagency interoperability. Second, this thesis suggests using an organization approaches by creating a networking cooperation model, followed by issuing operative legal guidance to enable the cooperation system to run more effectively within and among national cyber agencies.

Research Purpose

The author has three purposes in conducting research as described below:

1. this thesis is to observe the three key pillars of cyberspace activity in Indonesia;
2. this thesis is to analyze the urgency of a National Cyber Security Strategy and a National Cyber Security Agency;
3. this thesis is to analyze the urgency of interoperability interagency in achieving a national comprehensive approach by tailoring Indonesia interagency cyber cooperation and coordination system consisting of the three key pillars.

The end state of this thesis is to provide a description about how Indonesia should achieve a national cyber resilience capacity by integrating, harmonizing, and building a comprehensive approach to deal with the national and international levels of cyber threats.

Research Questions

This thesis will answer the primary question, “How to achieve Indonesia’s cyber resilience capacity by tailoring interagency interoperability?” Accordingly, this problem statement will be analyzed by several secondary questions (1) What are the ICTs’ role in Indonesia’s three key pillars of activity: economic, security, and governance? (2) What are the threats and risks associated with utilizing ICT or cyberspace? (3) What lesson learned can be obtained from international cyber organizations for enhancing Indonesia cyber resilience capacity? How did Indonesia establish a National Cyber Security Strategy? Finally, (4) How does the National Crypto and Cyber Agency of Indonesia perform as the main effort of government’s roles to achieve the National Cyber Security Strategy’s objectives; what are the potential challenges and how to mitigate them?

Assumptions

The author identifies several assumptions related to this thesis as described below.

1. ICTs play significant role in developing Indonesia’s economic, security and governance systems.
2. Indonesia cannot be excluded from the international, regional and national cyber threats and risks.

3. Indonesia has lesson learned from International cyber community by developing a National Cyber Security Strategy and a National Cyber Security Agency.
4. The Indonesia government plays the key role in achieving the National Cyber Security Strategy's objectives.
5. The new age of the transformed national cyber security agency is one of the major challenges for implementing national cyber security's strategic vision role to harmonize and synergize stakeholders in participating in national security and increasing national economic growth.
6. There are two possible solution to mitigate the challenges: leadership and organizational approaches.

Definitions

The following terms are crucial to comprehending the issues in this research discussion:

Cyberspace: consists of various and often overlapping networks, as well as the nodes (any devices or logical locations with an Internet protocol (IP) address or other analogous identifiers) on those networks, and the system of data (such as routing tables) that support them. Cyberspace can be divided in terms of three layers: physical network, logical network, and cyber-persona.¹⁴

¹⁴ U.S. Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: Government Printing Office, 5 February 2013), v.

Cybersecurity: the organizations and collections of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences which misalign *de jure* from *de facto* property rights.¹⁵

Moreover, cybersecurity is the gathering of tools, policies, security concepts, guidelines, security safeguards, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber organization and environment, and user's assets. Organization and user's components include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and stored information in the cyber environment.¹⁶

Cyber resilience: the capability to continuously perform the intended outcome despite adverse cyber events caused by humans and nature.¹⁷

Cyber-attacks: forms of actions, words, thoughts either intentionally or not intentionally by any party, with motives and goals, done at any location, which target

¹⁵ Dan Craigen, Nadia Djakun Thibault, and Randy Purse, "Defining Cybersecurity," *The Technology Innovation Management Review* (17 October 2014): 13-21, accessed 2 January 2019, <https://www.academia.edu/9061472/DefiningCybersecurity>.

¹⁶ The International Communication Union (ITU), *Series X: Data Networks, Open System Communications, and Security Telecommunication Security - Overview of Cybersecurity*, Recommendation ITU-T X.1205, 2 April 2008, accessed 9 February 2019, <https://www.itu.int/rec/T-REC-X.1205-200804-I>.

¹⁷ Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic, "Cyber Resilience –Fundamentals for a Definition," *Advances in Intelligent Systems and Computing* 353 (1 January 2015): 311-316, accessed 25 December 2018, https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition.

electronic systems or their contents (information) or equipment that relies heavily on technology and networks on any scale; on vital or non-vital objects in the military and non-military sphere, which threatens state sovereignty, territorial integrity and national safety..¹⁸

National Cyber Security: any efforts to maintain confidentiality, integrity, and availability of information and all supporting cross-sectoral facilities at the national level..¹⁹

Information of Communication Technology: is similar to Information Technology but stresses more on the communication system that integrates telecommunications components with wireless through link system; teleworking, smart grids, electric cars, e-books, smart control systems for buildings are a few examples of ICT solutions..²⁰

Digital economy: is a particular range of economic activities at the core of digitalization..²¹

¹⁸ The Ministry of Defense of Republic of Indonesia, *State Gazette of the Republic of Indonesia, No.1712- Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014* (Jakarta: The Indonesia Ministry of Law, 17 October 2014), 12.

¹⁹ Ibid.

²⁰ Ernst & Young, *The Role of Green ICT In Enabling Smart Growth in Estonia* (Tallinn: The Ministry of Economic Affairs and Communications of Estonia, 2012), accessed 25 October 2018, http://www.mkm.ee/public/Inno_18_GreenICT.pdf.

²¹ The International Monetary Fund, “Measuring the Digital Economy,” 28 February 2018, accessed 11 February 2019. <https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy>.

Critical infrastructure: assets, systems, and networks, physical and virtual which are very vital, where disruption to them has the potential to threaten security, the stability of the national economy, safety and public health or a combination.²²

Interoperability: is the ability of an IT system component to work with other IT system components without special effort on the part of the user. Interoperability becomes a quality of increasing importance for information technology products as the concept that “The network is the computer” becomes a reality.²³

Multi-agency cooperation interoperability: on the government level, the capability of an organization or discrete parts of the same organization, to exchange operational information and use it to inform their decision making.²⁴

National security: the capability of a nation to protect its internal values from external threats.²⁵ In 1990, Charles S. Maier, Professor of History at Harvard University, mentioned that “national security is best defined as the capability to control those domestic and foreign conditions that the public opinion of a given community believes crucial to enjoying its self-determination or autonomy, prosperity, and well-being.”²⁶

²² The Ministry of Defense of Republic of Indonesia, *State Gazette of the Republic of Indonesia*, No.1712, 12.

²³ Stephen Hufnagel, “Interoperability,” *Military Medicine* 174, no. 43 (May 2009), accessed 23 February 2019, https://academic.oup.com/milmed/issue/174/suppl_5.

²⁴ The National Policing Improvement Agency, *Guidance on Multi-Agency Interoperability* (Bedfordshire, UK: Association of Chief Police of Officer, 2009).

²⁵ Joseph J. Romm, *Defining National Security* (New York: Council on Foreign Relation Press, 1993), 5.

²⁶ *Ibid.*, 6.

The Group of Twenty (G20): a global forum comprised of twenty of the world's largest economies, focused on addressing global economic challenges. Its membership includes nineteen countries—Argentina, Australia, Brazil, Canada, China, Germany, France, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom and the United States—and the European Union.²⁷

Scope

This thesis is divided by five chapters: introduction, literature review, research methodology, analysis, and conclusion. In chapter four (analysis), the author emphasizes topic discussion by providing five key points:

1. ICTs' role in sustaining Indonesia's three key pillars of activity: economic, security, and governance.
2. Threats and risks which are associated with utilizing ICT or cyberspace.
3. Lesson learned can be obtained from international cyber communities and organizations for enhancing Indonesia cyber resilience capacity.
4. The establishment of Indonesia National Cyber Security Strategy.
5. The National Crypto and Cyber Agency of Indonesia's role to succeed the National Cyber Security Strategy's objectives. It includes the potential challenges associated with it and provides possible solutions to mitigate it.

²⁷ Alina Alimova and Nicholas Goggin, "The G20 Summit Explained," *Atlantic* (blog) *Atlantic Council*, 29 November 2018, accessed 2 February 2019, <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-g20-summit-explained>.

Limitations

Time constraint is one of the prevalent challenges in conducting this study. The availability of resources is also one of the issues because a cyber cooperation framework is a relatively new matter and has just been developing in many countries. Although this thesis discusses the strategic level in achieving cyber resilience capacity and capability, there would potentially be some classified information included; however, this thesis reflects and uses only unclassified open source information.

Delimitations

Adhering to the purpose, this thesis does not discuss all aspects of Indonesia cybersecurity strategy. As mentioned above, this thesis excludes discussing three other nomenclatures of cyber contemporary architecture in the National Cyber Security Strategy: cyber industries, scholars, and cyber communities. During discussing the government's roles, this thesis' content will also be absent from legal measures, for example, cybercriminal legislation, cybersecurity legislation, and training. Moreover, this thesis does not deeply discuss standards for organizations, professionals, and cyber security metrics. The author does not cover a technical process, technical measures and operations, and capacity building in achieving cyber resilience capacity. Therefore, there is no discussion about standardization bodies, cybersecurity good practices, research and development programs. Also, this thesis excludes a discussion about public awareness campaigns, professional training courses, education programs, incentive mechanisms, and home-grown industry. Finally, the author discusses the cooperation pillar but excludes intense observation about the public-private partnership aspect.

Significance of the Study

This study is significant because it is important to provide a body of knowledge which demonstrates and convinces government officials and other stakeholders of the need to achieve interagency interoperability. The author provides examples of how the Indonesian government has created the National Cyber Security Strategy that potentially provides a comprehensive approach of achieving the National Cyber Security Strategy's objectives.

CHAPTER 2

LITERATURE REVIEW

This chapter reviews references regarding how Indonesia can achieve cyber resilience capacity and capability. There some previous research available consisting of the government documents, international organization cyber assessments, books, journals, and some other open resources. This chapter primarily observes the five key points that being discussed in chapter four. Those are ICTs' role in economic, security and Indonesia governance; cyber threats; international cyber communities or organizations' report, and Indonesia's cyber cybersecurity elements.

First and foremost, ICTs perform significant roles in supporting Indonesia economic, security, and governance. Indonesia's national interest is upholding the Republic of Indonesia based on Pancasila (five principles of national ideology) and the 1945 Constitution as well as ensuring the sustainability of national growth to achieve national objectives..²⁸ Currently, Indonesia is moving toward a society that relies on the cyber capacity to achieve its growth and development encompassing national ends: to protect people and homeland security and promote prosperity.

The President of the Republic of Indonesia provides policy guidance for enabling cyber capacity to support economic growth. Indonesia has been promoting digital economics to leverage Indonesia economic growth adhered to national objectives and national interests. The Minister of Communication and Information asserted that

²⁸ The Ministry of Defense of the Republic of Indonesia, *Defense White Paper* (Jakarta: The Ministry of Defense of the Republic of Indonesia, 2015), 28.

Indonesia has already had “four unicorns,” companies that have reached billions USD in value without tapping the stock markets. This progress provides significant movement toward a digital society; the users generated the development of e-commerce that reached an income of USD 2.6 billion in 2014.²⁹ The Secretary-General of the Indonesian Internet Service Provider Association (APJII), Henri Kasyfi Soemartono, reported that more than 50 percent of the 262 million population, or around 143.26 million people, were connected to the internet by the end of 2017.³⁰ The amount of internet users in supporting digital economic movement provides evident that ICTs plays significant role in Indonesia economic growth.

The description of internet usage in Indonesia is like many countries around the world. Furthermore, they are similar to Amazon, JD.com, and Alibaba; on a smaller scale, ride-hailing company Go-Jek, similar to Uber, travel site Traveloka, and e-commerce Bukalapak and Tokopedia.³¹ These companies help citizens to communicate, meet their primary needs, order daily transportation, buy goods, and do business in convenient and efficient ways. Instances of cyberspace matters also incorporate daily activities. About 72.41 percent of users who live in urban areas are inclined to wait for

²⁹ Rachmatunnisa, “3 Tahun Jokowi-JK, Geber Ekonomi Digital Terinspirasi Silicon Valley.”

³⁰ Sakina Rakhma Diah Setiawan, “Tahun 2017, Pengguna Internet di Indonesia Mencapai 143,26 Juta Orang,” *Kompas*, 19 February 2018, accessed 11 August 2018, <https://ekonomi.kompas.com/read/2018/02/19/161115126/tahun-2017-pengguna-internet-di-indonesia-mencapai-14326-juta-orang>.

³¹ Ibid.

the internet morning alarms to wake up.³² People who live in Indonesia's capital city and all Java Island Provinces rely heavily on social media and internet texting services or applications to communicate; likewise, in Sumatra Island, Kalimantan, Sulawesi, Bali-Nusa, and Maluku-Papua. Students recheck their updated schedule, homework, or assignments from their peers. While people used to read morning newspapers, they now receive regular updates on their cell phones or tablets, allowing for more efficient reading and remaining informed on developing stories throughout the day. Others watch broadcasts on smart TVs. After arriving in ones' respective workplaces, many projects require cyberspace to carry out the work because there are abundant references available on the screen such as journals, e-books, and some others. Regardless of what ones' occupation and responsibility, cyberspace is ubiquitous. Technology has shifted the lifestyle of half of Indonesia's peoples, striving to reach their dreams.

However, the double-edged consequences of cyberspace matters are encountered by many countries in the world, including Indonesia. Internationally, there have been some previous research about the cyber threat at the international level. Several books titled, *Cybersecurity and Cyberwar-What Everyone Needs to Know*, *The Perfect Weapon*, *Digital Resilience-Is Your Company Ready for The Next Cyber Threat?* and, *Shaping the Future of the Fourth Industrial Revolution* provide illustrations about the worldwide cyber threats issues that potentially can affect national stability. Supported by other internet open resources, authors, and publications discuss the most current and sensitive

³² Sarah Yuniarni, "Indonesia Had 143M Internet Users in 2017: APJII," *Jakarta Globe*, 19 February 2018, accessed 6 November 2018, <https://jakartaglobe.id/business/indonesia-143m-internet-users-2017-apjii>.

of allegations of Russia's interference in the US election, WannaCry crossing the world, Stuxnet the worm virus in Iran, cyber-attack incident in Estonia and Georgia, and hospitals' cyber-attacks in Singapore and the United Kingdom. The 2017 Norton Cyber Security Insights Report suggests that in 3.1 billion populations of 20 countries researched, there were 57 percent connected to the internet and half experienced Cybercrime.

On the national level, the author references some information from journals and books to analyze the threats and risks associated with cyberspace. Cyber-attacks growth and expansions have challenged Indonesia. The Directorate General for Postal and Information Technology Affairs researched that in the period from January to mid-December 2014, the total attack data recorded by its monitoring system reached 48.4 million.³³ The Indonesia Security Incident Response Team on the Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) testified that Indonesia experienced around 42 thousand attacks per day.³⁴ The 2017 Norton Cyber Security Insights Report suggests that, within that year, about 59.45 million Indonesia adults experienced cybercrime with 34 attacks per three-days that caused victims to lose USD 3.2 billion.³⁵

³³ The Directorate General for Postal and Information Technology Affairs, *Annual Report* (Jakarta: The Directorate General for Postal and Information Technology Affairs, 2014).

³⁴ Id/SIRTI-CC, *Pasukan Cyber Indonesia Harus Dipimpin Presiden!* (Jakarta: Id/SIRTI, 2014), accessed 17 December 2018, <https://idsirtii.or.id/berita/baca/48/pasukan-cyber-indonesia-harus-dipimpin-presiden-.html>.

³⁵ Symantec, *The 2017 Norton Cyber Security Insights Report* (Tempe, AZ: Symantec, 2017), 14.

Moreover, Indonesia needs to enhance its cybersecurity awareness by leveraging developing efforts to encounter these threats that affect the national interest.

In analyzing approaches to mitigate those issues, the author uses some references from international organization research. Lessons learned from World Economic Forum's research, GCI 2017, Cyber Maturity in the Asia Pacific Region 2017, and National Cyber Security Index 2018 provide distinct challenges that might be encountered in leveraging Indonesia cyber resilience capacity by tailoring its interagency partnership. Those distinct challenges are the most concerned aspect in according to the existence of BSSN as the new-transformed organization assimilated by three different agencies, and how this agency as the center of national cyberspace cooperate with other agencies. GCI 2017 was published by the International Telecommunication Union (ITU) assessing 193 countries' cybersecurity level. Cyber Maturity assessment, in the Asia Pacific Region 2017, created by the Australian Strategic Policy Institute (ASPI) analyzes the country cyber maturity level. There are many other organization measurements that provide state cyber readiness level information and cybersecurity policy making points but will not be discussed in this thesis. Research from World Economic forum depicted on figure-9 (Key Barrier in Adopting the Industrial Internet) suggests the primary challenges for achieving interagency interoperability.

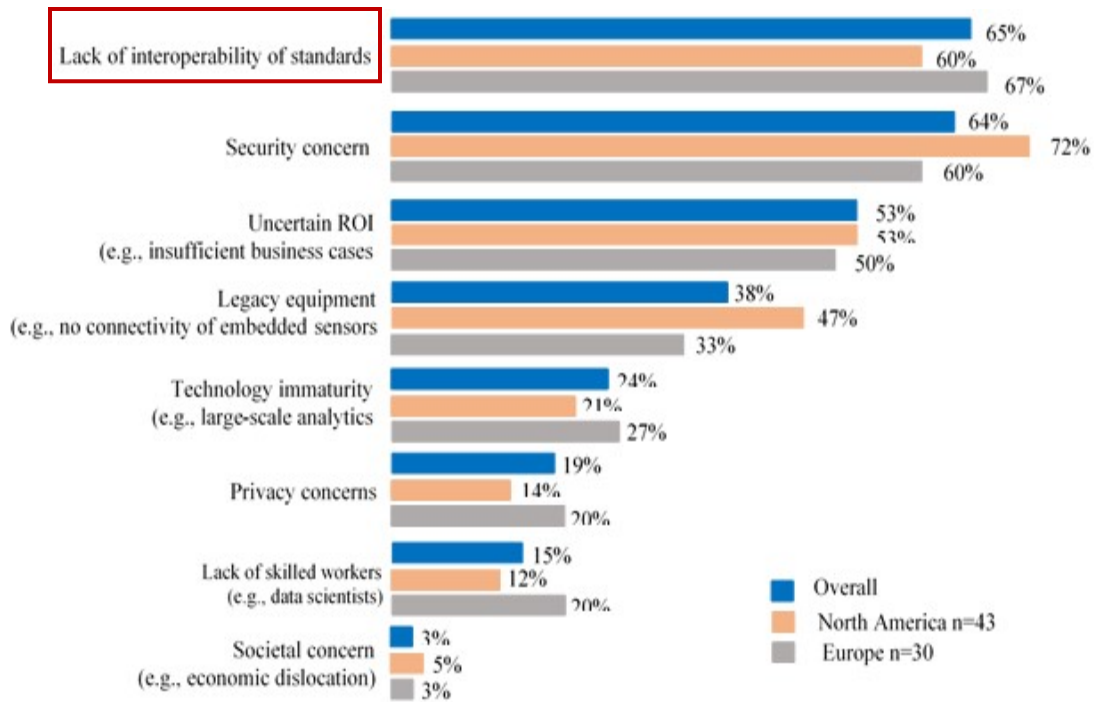


Figure 2. Key Barrier in Adopting the Industrial Internet

Source: World Economic Forum Survey (2014), quoted in Klaus Schwab and Nicolas Davis, *Shaping the Future of the Fourth Industrial Revolution, 2018* (Geneva, Switzerland: World Economic Forum, 2018).

GCI 2017 measurement system is based on the availability of national cybersecurity development strategy and policy for enabling agencies cooperation.³⁶ GCI 2017 defines that cooperation pillar reflects collaborative efforts encompassing national and international territories concerning the public and private sector.³⁷ This pillar has five considerations: bilateral agreements, multilateral agreements, international for a

³⁶ The International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva, Switzerland: ITU, 2017).

³⁷ Ibid.

participation, public-private partnerships, and interagency partnerships.³⁸ Interagency partnerships encompass any authorized cooperation amongst ministries, departments and agencies, excluding international collaboration aspect.³⁹

GCI 2017 argues that a national cyber strategy is a high priority demonstrating a robust commitment of a country to reach a high level of preparedness to respond to digital networks risks and threats. However, half of the 193 countries surprisingly have not yet established their national strategy, while 12 percent is under development, and 11 percent dedicates a standalone strategy. This thesis supports the urgency of a national cybersecurity strategy and provides suggestion for its implementation.

³⁸ Ibid.

³⁹ Ibid.

Table 1. Countries Index Cyber Assessment				
Name	Position Indonesia/Score	Research Method	Indicators	Top Positions (1 & 2)
Global Cybersecurity Index 2017	70 out of 193/ Score 0.424	Primary & Secondary By International Telecommunication Union (ITU)	5 pillars, 24 indicators	Singapore 0.92 The United States 0.91
Cyber Maturity in the Asia Pacific Region 2017	12 out of 25/ Score 54.3	Secondary By the Australian Strategic Policy Institute (ASPI)	10	The United States 90.8 Australia 88.0
National Cyber Security Index 2018	83 out of 100/ Score 19.48 with digital development level 50.22	Primary & Secondary By E-Government Academy (Estonia)	3 categories, 12 capacities 46 indicators	France 83.12/79.06* Germany 83.12/81.95*

Source: Created by author using data from The International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva, Switzerland: ITU, 2017); The Australia Strategic Policy Institute, *Cyber Maturity in the Asia-Pacific Region 2017* (Barton ACT, Australia: International Cyber Policy Centre, December 2017); E-Governance Academy (Estonia), *National Cyber Security Index 2018*, <https://ega.ee/>.

The table below shows the indicators examined. Following the purpose of writing, the subsequent writing underlines cyber agency interoperability aspects.

Table 2. Cyber Assessment Indicators		
Name	Pillars/ Capacity	Indicators
Global Cybersecurity Index 2017	a. Legal measures;	(1) Cybercriminal legislation (2) Cybersecurity legislation (3) Cybersecurity training
	b. Technical measures;	(1) National CERT/CIRT/CSIRT (2) Government CERT/CIRT/CSIRT (3) Sectoral CERT/CIRT/CSIRT (4) Standards for organizations (5) Standards for professionals (6) Child online protection
	c. Organizational measures;	(1) Strategy (2) Responsible agency (3) Cybersecurity metrics
	d. Capacity building;	(1) Standardization bodies (2) Cybersecurity good practices (3) Research and development programs; (4) Public awareness campaigns (5) Professional training courses (6) Education programmes (7) Incentive mechanisms (8) Home-grown industry
	e. Cooperation;	(1) Bilateral agreements (2) Multilateral agreements (3) International participation (4) Public-private partnerships (5) Interagency partnerships
Cyber Maturity in the Asia Pacific Region 2017		(1) Organizational structure; (2) Legislation/regulation; (3) International engagement; (4) CERTs; (5) Financial crime; (6) Military role in cyberspace; (7) Govt–business dialogue; (8) Digital economy; (9) Public awareness; and, (10) Internet connectivity.
National Cyber Security Index 2018	a. Legal act b. Established unit c. Official cooperation format d. Outcomes/Products	(1) Policy. Cybersecurity policy development (2) Threats. Cyber threats analysis and informing (3) Education. Education and professional development (4) Global. Contribution to global cybersecurity (5) Digital. Protection of digital services (6) Essential. Protection of essential services (7) eID & TS. E-identification and trust services (8) Personal. Protection of personal data (9) CIRC. Cyber incidents response 24/7 (10) Crisis. Cyber crisis management (11) Police. Fight against cybercrime (12) Military. Military cyber operations

Source: Created by author using data from The International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva, Switzerland: ITU, 2017); The Australia Strategic Policy Institute, *Cyber Maturity in the Asia–Pacific Region 2017* (Barton ACT, Australia: International Cyber Policy Centre, December 2017); E-Governance Academy (Estonia), *National Cyber Security Index 2018*, <https://ega.ee/>.

Based on prior researches, the author analyzes the Indonesian government's effort in achieving national resilience capacity. The Indonesian government pronounced the Indonesia Cyber Security Strategy in June 2017. The National Cyber Security Strategy provides a strategic guidance of cybersecurity policy providing a framework to internally build a deterrent effect through system and power development and promote the omnidirectional policy to increase interoperability among government agencies, cyber industry, scholars, and cyber community.⁴⁰ Referring to its strategic vision to establish and sustain national cybersecurity capability by various synergizing stakeholders to participating in national security and increasing national economic growth; there are five basic principles of this strategy encompassing sovereignty, independence, security, togetherness and adaptability, to achieve the strategic vision of Indonesia cyber strategic strategy.⁴¹ These efforts are intended to achieve cyber resilience capacity and capability by simultaneous and intense unity of efforts of all national critical elements.

⁴⁰ Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

⁴¹ BSSN, "Remarks the Chief of BSSN about Indonesian National Cyber Security Strategy."

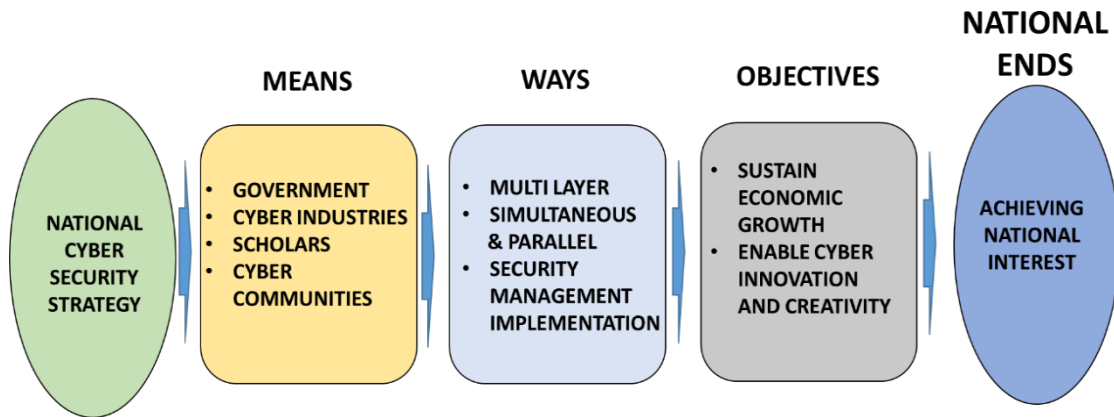


Figure 3. Indonesia National Cyber Security Strategy Framework

Source: Created by author.

The government is the primary means for achieving the National Cyber Security Strategy's objectives. Accordingly, the Indonesia Cyber Security Strategy highlights the government's roles in leveraging national cyber strategy consisting of protecting the national cyber environment, national e-Commerce, national critical information infrastructure, controlling penetration in regards to ideology, politics, social concerns, cultures, and national defense and security, and protecting citizens as well as their privacy.⁴² Besides those roles, the government is also required to conduct capability development programs including cyber intelligence, cyber defense, cybercrime, cyber diplomacy, and cyber economy. Both the government's roles and capability development programs are depicted on Table 3 and 4.

⁴² BSSN, *Strategi Keamanan Siber Nasional*.

Table 3. Government's Roles	
1	Protecting the national cyber environment,
2	Protecting national e-Commerce,
3	Protecting national critical information infrastructure,
	• Government
	• Defense and Security
	• Banking
	• Health
	• Energy and Mineral Resources
	• Transportation
	• ICT
	• Food security
4	Control penetration concerning ideology, politic, social, cultures, and national defense and security
5	Protecting Citizen / Privacy

Source: Created by author using data from Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

Table 4. Government Development Program

1	Cyber intelligence
2	Cyber defense
3	Cybercrime

Source: Created by author using data from Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

The National Cyber and Crypto Agency - *Badan Sandi dan Siber Nasional* (BSSN) is the government's main effort to achieve the National Cyber Security Strategy's objectives. BSSN is the new establishment of the national strategic cyber agency, created in May 2017 through Presidential Regulation no. 53/2017 and 133/2017. This agency is led by a head of the agency, under, and responsible to the President

through ministers that coordinate, synchronize and control the administration of political, legal and security affairs. BSSN is tasked to prepare, implement, monitor, and evaluate technical policies, coordinate ministries, institutions, and agencies on cybersecurity substances, and coordinate regional and international relationships.

BSSN's core mission is to run effective and efficient cybersecurity by utilizing, developing, and consolidating all elements related to cybersecurity.⁴³ It has two main functions as below:

1. Conducting preparation, implementation, monitoring and evaluation of technical policies in the field of identification, detection, protection, countermeasures, recovery, monitoring, evaluation, control protection electronic-based trading, coding, screening, cyber diplomacy, cyber management crisis, information centers, mitigation support, recovery of vulnerability, incident and / or cyber-attack.
2. Coordinating functional activities in implementing the task of the BSSN and as a forum for coordination for all stakeholders; implementation of substantive support to all organizational elements within the BSSN, national, regional, and international in cybersecurity matters.

Furthermore, this chapter reviews potential concerns for the Indonesian government to implement the national cyber security strategy. There are two significant concerns that are related to internal matters and external issues. The new age of the

⁴³ Badan Siber dan Sandi Negara (BSSN), *Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2018 Tentang Organisasi Dan Tata Kerja Badan Siber Dan Sandi Negara* (Jakarta: BSSN, 2018).

national cyber security agency and networking/coordination system with other agencies are the internal concern. On the other hand, the external concern is regarding the expansion of cyber threats and risks associated with it. Based on that view, there are some potential solutions for addressing the challenges. The author assumes that tailoring cooperation interagency is the primary requirement for internal and external challenges. John P. Kotter's model about leading change, focusing on the coalition guidance and his research about culture and commitment of new organization, is a primary reference for identifying issues related and providing ways for addressing it.

All in all, this thesis observes references from many types of resources. It analyzes primarily the issues regarding cyberspace utilization emphasizing cyber threats and risks. It perceives some references from international assessment of cyberspace interoperability challenges and key requirements to achieve that. Finally, it assumes the challenges associated with that approaches observing Indonesia interoperability environment and recommends possible ways for mitigating that.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter describes how the author formulates a method to provide a broad concept about cyber situation environment in Indonesia that can support it to achieve cyber resilience capacity. The thesis uses a qualitative analysis approach based on non-numerical data, information from the literature review, and limited information based on personal experience. The author uses Army Design Methodology (ADM) as the primary way to identify what current conditions, desired conditions, frame the problems, develop a problem-solving strategy, and develop a plan depicted by questions below:

1. What is going on in the environment?
2. What do we want the environment to look like?
3. Where—conceptually—should we act to achieve our desired state?, and what is the problem
4. How do we get from the current state to our desired state?

The author identifies the cyber environment in Indonesia by describing the following conditions. Current condition describes the ICT role in Indonesia and threats associated with cyberspace. Then, it is followed by observing lesson learned from international organizations' cyber assessment to analyze Indonesia's approach to achieve cyber resilience capacity.

The existence of the National Cyber Security Agency Strategy (BSSN) created in 2017 is the primary requirement for achieving national cyber resilience capacity. While describing this subject, the author emphasizes the significant impact if Indonesia succeeds in implementing this strategy and describes national environment that can

enable the success of this strategy. The National Cyber Security Strategy also highlights the government's roles in achieving this strategy supported by its cyber development program. Specifically, the author observes the development of the National Cyber Security Agency (BSSN). How it can be operated effectively as a newly formed agency and how it can cooperate with other ministries and other national agencies to collaboratively achieve the National Cyber Security Strategy's objectives. Moreover, the author identifies the problems or challenges that potentially are faced by BSSN while achieving the desired condition and potential ways to mitigate those issues.

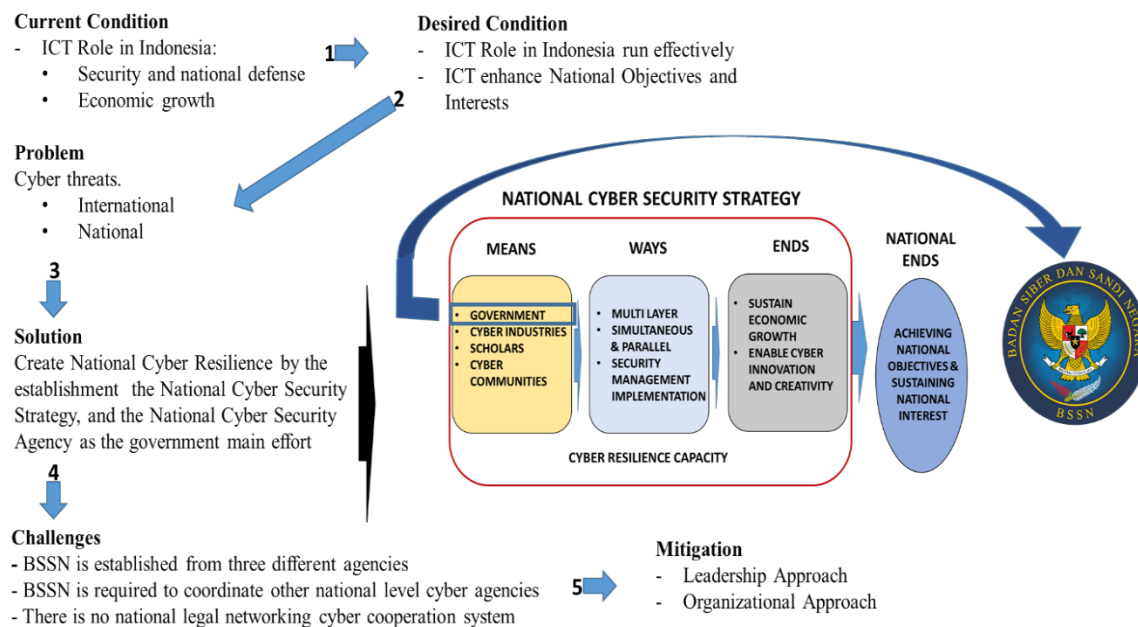


Figure 4. Research Methodology Portrayal

Source: Created by author.

As illustrated on Figure 4, the author highlights four core discussions. First, the government's roles in enhancing national cyber strategy encompassing ministries and departments that have roles in enabling current interoperability system and observe national and limited capability to achieve that. Second, the need of a cooperation and coordination networking model among the existing cyber agencies that enable the government's roles. It enhances the government's understanding of mapped network following conducting cooperation with the third party. Third, the need of a robust direction and regulation to commence the implementation of that interoperability system. It is necessary to develop a regulation to provide a legal partnership and coordination framework to enable an effective and efficient cooperation system inter cyber agencies.

Overall, this thesis analyzes issues regarding ICTs' role after providing information about its contribution for Indonesia's developments. This thesis observes international organization cyber assessment to analyze Indonesia's approach to achieve cyber resilience capacity and how Indonesia interprets those recommendations. Finally, this thesis analyzes potential challenges associated with those approaches and recommends solutions for addressing expected challenges.

CHAPTER 4

ANALYSIS

Information and Communication Technology's Role in Indonesia

Information and Communication Technology (ICT) has significantly been contributing to Indonesia's growth and development. For decades, the Indonesia government has put many efforts into its enhancement to protect nation and prosper the people. Indeed, combination technology and human can create a more effective system for both in the defense and security also in the economic sectors. This sub-chapter describes the current and desired situation of security and defense and economy that moves towards the enhancement of cyberspace reliance environment.

ICTs' Role in Leveraging National Defense and Security

National defense and security are the primary concern to enable and sustain national development projects to achieve national goals. It is the result of an environment that enable cyber innovation and creativity to create that end. ICTs that cannot be separated from cyberspace is one of the most effective means to acquire the national defense and security system. It provides a synchronized and integrated system to enable a country protecting its territory; in this thesis is Indonesia.

Indonesia is the largest archipelago country in the world. It is located in a strategic position between the Pacific and India Oceans with more than 260 million people living on 17,500 island-country. It needs to be protected from both local and alien adversaries. For doing so, synchronized and integrated systems are essential to achieve a unity effort, and it is also needed to enhance national growth simultaneously. Besides its

world's paramount maritime biodiversity and utmost terrestrial biodiversity, Indonesia has a strategic role in the Pacific region. One example that portrays Indonesia's role in global power is its adjacent to the South China Sea, the world's busiest sea lanes. This sea lane passes a half of the world's oil tankers every year in an amount of over five trillion USD, and one of the most economic strategic sea lines of communications (SLOCs).⁴⁴ Scholars predict that Beijing's economic upsurge also affects Indonesia's rise portraying competition between the United States and China in the Pacific Region.⁴⁵ This situation can potentially impact Indonesia's geopolitical environment because US-Chinese current relationship echoes of that occurred between US and USSR during cold war.⁴⁶ Since 2011, the Pentagon's operation and strategy, by creating Cyber Command, has been undoubtedly reflecting China as the most threats.⁴⁷ besides being a strong competitor in one aspect of national power, which is economic power.

The Indonesia Ministry of Defense has performed a significant role in supporting national cyber defense capacity. The Ministry of Defense possesses a unit that purposes to secure all electronic systems and information networks in its stakeholders and to

⁴⁴ U.S. Department of State, Bureau of East Asian and Pacific Affairs, "U.S. Relations with Indonesia," Fact Sheet, 14 August 2018, accessed 30 January 2019, <https://www.state.gov/r/pa/ei/bgn/2748.htm>.

⁴⁵ Fels, *Shifting Power in Asia-Pacific?*, 697-698.

⁴⁶ P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar - What Everyone Needs To Know* (New York: Oxford University Press, 2014), 138.

⁴⁷ Ibid.

support the necessary coordination of cybersecurity in other sectors..⁴⁸ To achieve that objective, this unit has functions to ensure cyber defense policy targets and purposes, build the organization and governance's cybersecurity, and perform deterrence effects of cyber risks and threats. In the international and regional level, this agency has been performing cooperation and coordination to achieve cyber defense capacity building..⁴⁹ Those purposes, functions, and activities allow Indonesia to achieve cyber resilience and create an awareness environment.

Moreover, the ICTs contributes development of military and cyber defense capabilities. ICT promotes the establishment of military cybersecurity, cyber defense, cyber army, navy, air force, and strategic electronics and technology defense. In 2016, the Australian Strategic Policy Institute (ASPI) stated how Indonesia's understanding of cyberspace sustaining integrated support for military operations, as an asymmetric weapon for non-linear warfare, depicted in Indonesia Defense White Paper. In 2017, ASPI highlighted the Indonesia military's developing role in cyberspace, cyber policy, and cybersecurity portraying military leaders' commitment to deny cyber narcoterrorism and influence soldiers including the online spread of false news. ASPI also underlines the Indonesian National Armed Forces cyber unit establishment and development. It includes missile tracking, satellite surveillance, and defending networks in electronic and information warfare. That establishment might portray the embryo of defense cyber development in Indonesia.

⁴⁸ The Ministry of Defense of the Republic of Indonesia, *State Gazette of the Republic of Indonesia*, No.1712.

⁴⁹ Ibid.

Furthermore, ICT promotes law enforcement's scheme in achieving cyber resilience capacity. Cyber systems facilitate efforts to create a trustful reformation of law enforcement system in law and justice, fighting corruption, deterring illegal logging, battling narcotics and drugs, supporting land rights, and protecting women and marginalized groups' rights encompassed in the National Mid-term Development Plan. For example, Indonesia National Police enhances their cyber capacity, through its cyber-crime unit that was previously created based on the Chief of National Police's Decree on October 17, 2002. Polices are facilitated by cyberspace to ease mission accomplishment regarding cyber-crime and non-virtual lawbreaking that can be solved by any kinds of physical objects that is connected and operated in the cyberspace. The Indonesia National Police has a role to conduct special criminal act investigation related to information technology, telecommunications, and electronic transactions.⁵⁰ There are several functions related to electronic transactions investigation such as carding, money laundering, capital markets, taxes, and banking issues. As a tool, the Indonesia National Police' role requires capability of investigating cases related to communication and information technology including telephone tapping, misuse of VoIP, and fraud through mobile phones. Indonesia law enforcement departments are prepared to observe the misuse of internet facilities such as cyber gambling, cyber terrorism, cyber fraud, cyber pornography, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber threatening, data theft, insulting, and defamation. The law enforcement units will observe and examine the illegal system, DDOS attack, hacking, tracking, hoax news, and

⁵⁰ The Indonesia National Police, *The Indonesia National Chief of Police' Decree of number 54 / X / 2002* (Jakarta: The Indonesia National Police, 17 October 2002).

creating and distributing destructive properties, malicious code all viruses such as worms, rabbits, trojans. They have power to conduct ongoing crime investigations related to Intellectual Property Rights (IPR), pirated software, voice recording and website. The Australian Strategic Policy Institute (ASPI) highlights Indonesia law enforcement emergence to support a robust capability through its partnership with other agencies. Supported by financial misconduct investigations, Indonesia exposed the online fraud syndicate targeting businesspeople and politicians in an amount of 450 million through 2017 USD.⁵¹ Collaboration with Ministry of Foreign Affair, Indonesia law enforcement participated in many ASEAN, Interpol, and regional seminars.

In protecting its territory, Indonesia has also been strengthening its relationship with regional and international nations. Indonesia has been performing a significant role in its region as a founding member of ASEAN - promoting it becoming Global Community of Nations - and the East Asia Summit; a member of the United Nations participating in United Nations peacekeeping missions, the World Trade Organization (WTO) and OPEC; a founding member of the Non-Aligned Movement (NAM) and the Organization of Islamic Cooperation (OIC). As the most populated Muslim-majority country and a member of the Organization of Islamic Cooperation (OIC), Indonesia promotes Islamic solidarity and moderation of Islamic countries by constructing the world's third largest democracy;⁵² Since President Yudhoyono's power in office,

⁵¹ The Australia Strategic Policy Institute, *Cyber Maturity in The Asia-Pacific Region 2017* (Barton ACT, Australia: International Cyber Policy Centre, December 2017), 32, 41.

⁵² U.S. Department of State, "U.S. Relations with Indonesia."

Indonesia has been leveraging its position as a middle power in more than a few eminent forums, for example, as ASEAN representative in G20 forum. During Joko Widodo Presidency, Indonesia stunningly organized the 18th Asian Games and remarkably succeeded in becoming the host of the 2018 World Bank Group Events annual meeting.⁵³

The Indonesia Ministry of Foreign Affairs has performed a significant role in promoting ICTs. This ministry had been facilitating the enhancement of the use of the internet by promoting international cyber cooperation to support economic growth, as well as national security and defense through cyber diplomacy.⁵⁴ Cyber diplomacy provides national cyber strategy, a diplomatic tool to discuss and answer cyber risks and threats.⁵⁵ In a broader dimension reaching international level, cyber matters are its concern or end state, while digital diplomacy or diplomacy itself is a mean that links as a tool to achieve the objective.⁵⁶ The topics discussed vary encompassing cyber digital of governance, implementation of regulation related cybercrime, and cyberspace' flexibility to encounter malicious attacks as the primary concern of cyber resilience. Cyber

⁵³ The World Bank, Remarks by World Bank Group President Jim Yong Kim at the 2018 Annual Meetings Plenary, Jakarta, 12 October 2018); Indonesia Travel, "18th Asian Games A Resounding Success: Indonesia Praised Worldwide," 6 September 2018, accessed 23 December 2018, <https://www.indonesia.travel/us/en/news/18-th-asian-games-a-resounding-success-indonesia-praised-worldwide>.

⁵⁴ Carmen Elena Cîrnu, "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy," *The Market for Ideas*, September-December 2017, number7-8, accessed 10 February 2019, <http://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/>.

⁵⁵ Ibid.

⁵⁶ Ibid.

diplomacy also includes discussion and agreement for the protection of national critical infrastructures.⁵⁷ It promotes bilateral agreement, transfer of technology, and capacity building.

Indonesia cyber diplomacy also can be observed from the Cyber Desk's activities. The Cyber Desk is part of Ministry for Political Legal and Security Affairs by which its minister will be handed over to BSSN.⁵⁸ Since it was established January 2014, Cyber Desk has been supported by the Ministry of Foreign Affairs primarily to promote and coordinate the cybersecurity system in Indonesia at the national, regional, and international levels. It promoted bilateral agreement, transfer of technology, and capacity building. There has been a considerable number of cooperation indicators in the cyber assessment index being executed by this agency. Cyber Desk participated in the Cyber Security Policy Course (CSPC) in 2014, Black Hat 2014 and Black Hat 2015, and International Cyber Security Visitor Leadership Program 2015 arranged by the United States. It also cooperated with Singapore in ASEAN Regional Forum (ARF) on Cyber Security 2014, Cyber Security Agency (CSA) 2015, and ASEAN Cyber Confidence Building Measures 2015. This agency's participation includes many cyber networking activities and conferences in the world in South Korea, Finland, Netherland, Swiss, India, Japan, Malaysia, and many other international events.

⁵⁷ Cîrnu, "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy."

⁵⁸ The Coordinating Ministry for Political Legal and Security Affairs of Republic of Indonesia, *Menko Polhukam dan BSSN Bahas Sinergitas Siber* (Jakarta: The Coordinating Ministry Polhukam Public Relation Bureau, 21 January 2018).

Furthermore, the Indonesia cyber diplomacy element succeeded to build bilateral and multilateral cyberspace cooperation. Indonesia signed a memorandum of understanding (MoU) as a bilateral agreement with the United Kingdom to enhance cyber awareness and achieve an apportioned cyber readiness level. ASPI also cited Indonesia's bilateral cyber meetings with Australia, Japan, and China. Indonesia has built bilateral cooperation on countering cyber-related extremism with Singapore, in addition to a trilateral treaty with the Philippines and Malaysia regarding a similar issue in Marawi. Other Id-SIRTII's contributions are participating in an agreement with India, Interpol, and ASEAN besides strengthening a relationship with Australia in cyberspace matters.

For the description above, readers can identify how Indonesia has been exerting cyber capability to enhance its national defense and security, and willing to enhance that capacity in interoperability systems. Therefore, the most highlighted concern is how these institutions can work together effectively in implementing cyberspace to obtain the higher value of efforts in protecting this nation. Besides, there are several other national agencies to protect national maritime assets, such as the Ministry of Maritime Affairs and Fisheries, the Coast Guard and the Navy. The Air Force is indeed the main component to protect the nation's air sovereignty that needs synchronization and collaboration information technology system with its counterpart. As the Indonesia location is on the world ring of fire, Indonesia is vulnerable to national disasters such as tsunamis, volcanoes, and floods. As a country with flourishing forest biodiversity, Indonesia has experienced peak forest fires that impact national and regional air pollution. It is not yet observing man-made disasters such as flight crashes, fires, and many others. There is a huge necessity to have a national

effort to overcome such situations; however, integrated and synchronized systems and efforts are not an easy matter.

ICT's role in Supporting National Economy

By going digital, Indonesia can unleash the next level of economic growth—to the tune of USD 150 billion in annual economic impact by 2025.

—Priyanka Sudhir, and Khoon Tee Tan,
Unlocking Indonesia's Digital Opportunity

Economic growth needs cyberspace-based technology. World Economic Forum in 2015 suggested that in the next 10 years (around 2025), cyberspace rapid development will intensely change industrial, energy, agronomy, transport and other manufacturing areas of the economy which, all those being mentioned, accounted to close to seventy-five percent of the global gross domestic product (GDP).⁵⁹ Those conditions will alter how an industrial system works in relationship to individuals and technologies. To observe that situation, the author describes current Indonesia economic situation and cyberspace's contribution in achieving national economic growth.

Acknowledging Indonesia Economic Development

Indonesia is considered as one of the six Middle Power economies.⁶⁰ The Indonesian economy has fully recovered from the 1997/98 economic crisis and is currently growing at a healthy pace. The improvement in economic conditions has brought Indonesia into the G-20 countries group. Furthermore, based on purchasing

⁵⁹ The World Economic Forum, “Industrial Internet of Things: Unleashing the Potential of Connected Products and Services” (Industry Agenda, Geneva, January 2015).

⁶⁰ Fels, *Shifting Power in Asia-Pacific?* 697-698.

power parity approach, Indonesia is currently the eighth-largest economy in the world. The prospect of the Indonesian economy is likely to remain bright. This is suggested by the Danareksa Research Institute business cycle indicators (Coincident and Leading Economic Indices).

The data in Figure 5 portrays Indonesia's business and economic cycle from January 1990 to April 2016. The indicators show that the Indonesian economy survived the 2008 global economic crisis. Despite the slowdown in that year, the economy rebounded quite fast. As such, the recession in 2008 was very mild. Please note that the length of the business cycle is about around seven years although there were some insignificant exceptions in some recession periods. Moreover, the Indonesian economy started to expand again in the first quarter of 2009. Theoretically, the Indonesian economy should have fallen into recession again in 2017. However, good fiscal and monetary policy prevented the economy from falling into a recession that year. Indeed, in mid-2015 the Indonesian government managed to create an early turnaround. The economy currently stays firmly in its expansionary path. This expansion is very likely to continue until at least 2023.

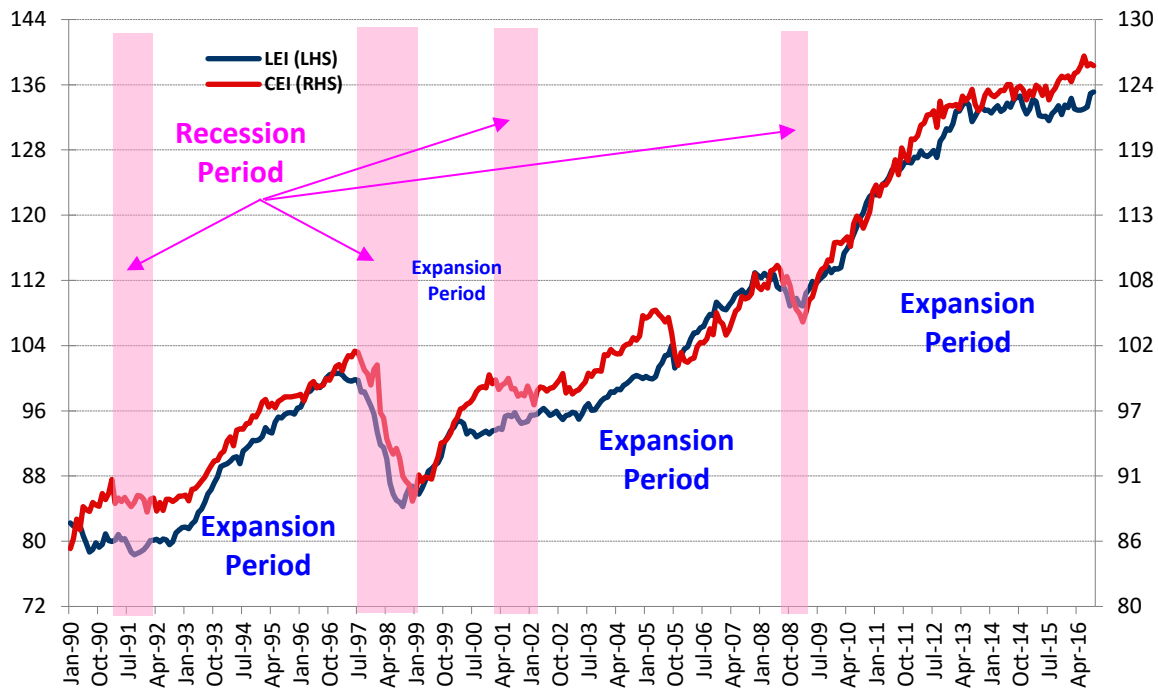


Figure 5. Indonesia Economic Growth (1990-2016)

Source: Purbaya Yudhi Sadewa, *Indonesia's Business and Economic Cycle* (Jakarta: Danareksa Research Institute, 12 January 2018).

Regional and International ICT Development: Indonesian's Economic Perspective

Cyberspace development in the region and international life affects Indonesian's perspective about cyber. Many countries in the world have been competing in the virtual world to support their economic growth. Those cyber advances include Information and Communication Technology (ICT) development in ASEAN, robotic systems around the world, and even the smart society notions in Japan.

ICT growth is obvious; and ASEAN, where Indonesia is, is the most prolific developers and users of this technology. ASEAN has the most internet users in the world;

in 2017, of the 2.1 billion internet users in the world, 922 million were part of ASEAN.⁶¹ It is predicted to increase since ASEAN is the largest regional organization in the Asia Pacific, and cyberspace economic and market interactions are also large in this region. Many infrastructure developments have been established supported by ICT systems such as transportation, mining, energy, banking, and telecommunication.⁶² Digitalization contributes a significant positive growth for national, regional, and international level.

Many countries around the world are looking forward to how robotic systems can leverage industrial technology. Currently, many of the biggest industries utilize robotic systems with AI to improve industrial production.⁶³ In developed countries, robots also are being advanced to travel to Mars and perform professional crafts like journalism, medicine, finance, and law.⁶⁴ Approximately half of the United States' labor connected to computerized robotic machines and Foxconn in China replaced more than sixty thousand workers with robots in factories over a two-year term.⁶⁵ Overall, the impact of a cyber-role in the industry is significant.

⁶¹ European Commission, *Accompanying the Document Proposal for a Directive of the European Parliament and the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union*, Impact Assessment (Strasbourg: European Commission, 7 February 2013).

⁶² Caitríona H. Heintz, *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime* (Washington: National Bureau of Asian Research, July 2014), 135.

⁶³ Klaus Schwab and Nicolas Davis, *Shaping the Future of the Fourth Industrial Revolution* (Geneva, Switzerland: World Economic Forum, 2018), 123.

⁶⁴ *Ibid.*, 128.

⁶⁵ *Ibid.*, 129.

Furthermore, regional curiosity of cyberspace's benefit is continuously increasing. This situation can easily be described by providing an example of the idea of "society 5.0" in Japan, conveyed by Japan Business Federation, Keidanren, in April 2016. They introduced an advanced society and manufacturing by integrating fourth industry revolution inventions such as the Internet of Things, big data, artificial intelligence (AI), cyber-physical system, and sharing economy.⁶⁶ The expected society 5.0 is a highly intelligent society; however, it demands a considerable commitment with complex and complicated processes. The first wall is a formulation of national strategies and integration from the government and agencies. Second, that expected society needs deregulation to facilitate the reformation of digitalization in the legal system. Third, it demands a knowledge foundation of technology to transform the cyberspace to robotic, nano, bio, and system technology. Fourth, this society must be managed by highly skilled professionals in cybersecurity and data science. Overall, this effort must be feasible, accountable and, the most important, accepted by society.

⁶⁶ Keidanren (Japan Business Federation), *Toward the Realization of The New Economy and Society - Reform of The Economy and Society by The Deepening of "Society 5.0"* (Tokyo: Keidanren, 28 April 2016), accessed 9 January 2019. http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf.

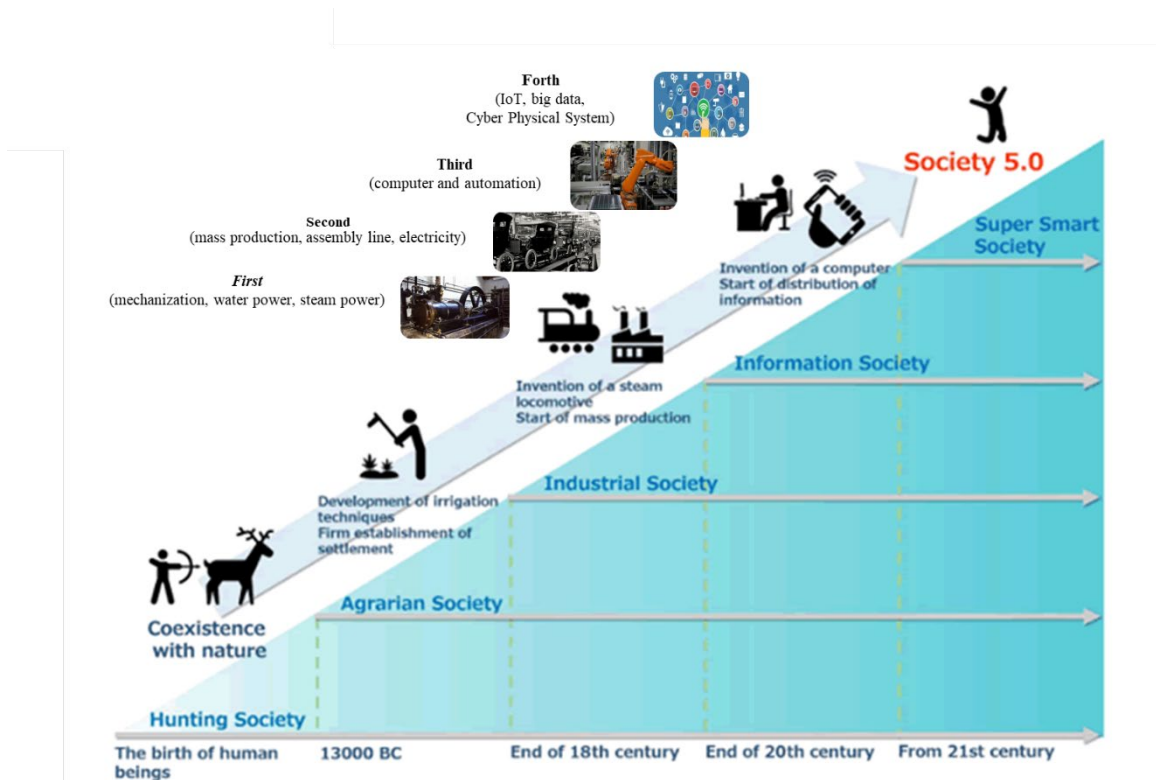


Figure 6. Revolution Industry and Evolutionary Aspect of the Society 5.0

Source: Keidanren (Japan Business Federation), *Toward the Realization of The New Economy and Society - Reform of The Economy and Society by The Deepening of "Society 5.0"* (Tokyo: Keidanren, 28 April 2016). Modified by author.

Those are examples of international and regional movement. There have been numerous countries facing digital transformation. These countries assertively enhance their speed of economic growth by relying on infrastructure and technology evolution. By and large, that situation affects Indonesian's perspective of cyberspace as one of the impacts of globalization.

Impact of Cyberspace for the Future Indonesia Economic Development

Regional and international ICT development has been shifting Indonesia economic perspective. Indonesia acknowledges the advantages offered by advancing economic sectors utilizing digital economic offered by international and regional cyber evolution. The author analyzes Indonesia digital economic system and its impact for small medium enterprises and economic life-style.

The Indonesia government has been increasing the national digital economic system. Global Connectivity Index (GCI) 2018 develops a mapping of new growth digital economy transformation. It has been researched that, currently, the digital economy contributed almost a fifth of global GDP, 12.9 trillion USD.⁶⁷ The digital economic remarkable contribution fascinates country to enhance driven-internet digital economic by enhancing, E-commerce, online services, and many kinds of entertainment.⁶⁸ E-Commerce system, for example, the advanced way of the economic transaction process, has become eminent not only in the rich country, but also in developing country due to its efficient and comfortable services. This is one of the paths to support the vision of making Indonesia “the digital energy of Asia.” By having a benefit offered by this system, the government, through the Ministry of Communication and Information,

⁶⁷ Huawei Technologies Co., “Global Connectivity Index 2018: Tap into New Growth with Intelligent Connectivity,” 2018, 24, accessed 25 December 2018, https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180914.

⁶⁸ Ibid.

launched startups for the digital economy.⁶⁹ In June 2016, the Indonesian President issued a thousand startups movement initiative aiming to boost startups growth reaching that number by 2021 with a total estimated economic value reaching ten billion USD.⁷⁰

Additionally, digital technology and e-commerce expectantly facilitate Small to Medium Enterprises (SMEs) to expand their economic reach and integrate into a formal economy without confronting long bureaucratic board challenges. The Ministry of Trade's launching of the Indonesia most-current online registration platform will relieve the long period issuance of business authorizations to support Indonesian economic growth.⁷¹ Echoing to that effort, the Minister of Communication and Information also has been encouraging youths and enterprises to create innovatively online commerce system to enhance economic growth. The Minister proudly pronounced that Indonesia has already had "four unicorns," companies that have reached \$1 billion in value without tapping the stock markets. Those include ride-hailing company Go-Jek, travel site Traveloka, and e-commerce Bukalapak and Tokopedia.⁷² At the end, these approaches help both companies and people (consumers) because they can easily communicate to

⁶⁹ Anggraini, "Indonesia's Vision: 1,000 Startups by 2020."

⁷⁰ Ambika Chopra, "Sustainable Tourism, Startups, and Innovation: A Glimpse into Indonesia Startup Weekend," Inc42, 8 June 2017, accessed 1 February 2019, <https://inc42.com/indonesia/startup-weekend-indonesia/>

⁷¹ G20 Germany 2017, *2017 Growth Strategy –Indonesia*, accessed 15 January 2019, https://www.bundesfinanzministerium.de/Content/DE/Downloads/G20-Dokumente/Hamburg_Wachstumsstrategien/IDN-Growth-Strategy.pdf?__blob=publicationFile&v=4.

⁷² Ibid.

meet their primary needs, order daily transportation, buy goods, and do business in convenient and efficient ways.

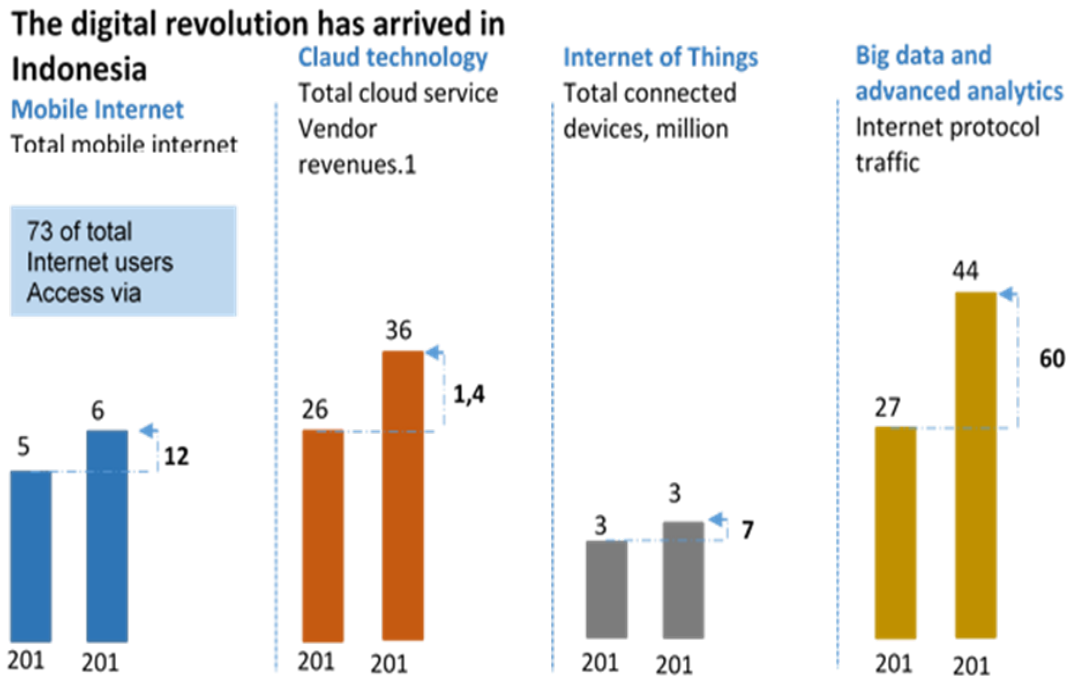


Figure 7. The Digital Revolution Has Arrived in Indonesia

Source: WCIS, Machina, IDC Worldwide Public Cloud Services and Cloud IT Infrastructure Tracker, World Robotics Report, quoted in Kaushik Das, Michael Gryseels, Priyanka Sudhir, and Khoon Tee Tan, “Unlocking Indonesia’s Digital Opportunity,” McKinsey & Company, October 2016, accessed 25 April 2019, https://www.mckinsey.com/~media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx, 5.

NOTES: 1. Revenues from public cloud services and cloud IT infrastructure.

2. 1 petabyte equals 1 million gigabytes.

Therefore, unsurprisingly, cyber technology has been shifting the Indonesian lifestyle and makes Indonesia as a country that has a considerable number of cyberspace

users. The Secretary-General of the Indonesian Internet Service Provider Association (APJII), Henri Kasyfi Soemartono, reported that more than 50 percent of the 262 million population, or around 143.26 million people, were connected to the ICT technology by the end of 2017.⁷³ The users generated the development of e-commerce that reached an income of USD 2.6 billion in 2014.⁷⁴

APJII also reported on the great variety of internet users. For example, 49.52 percent of the millennial generation, people born in the 1980s and 1990s, rely on the internet to support their daily lives.⁷⁵ This group includes new professions in the virtual domain such as Selebgram (Instagram celebrities) and YouTuber (YouTube content creators). The escalation of digital startup companies is also more or less driven by this age group, whether they are founders or consumers. This group also occupies the highest percent of the workforces in many government agencies, private businesses, and industry sectors. Users above millennials, up to 54 years, is the second level at 29.55 percent.⁷⁶

⁷³ Rachmatunnisa, “3 Tahun Jokowi-JK, Geber Ekonomi Digital Terinspirasi Silicon Valley.”

⁷⁴ Ibid.

⁷⁵ The Ministry of Communication and Information Technology of Republic of Indonesia, *Jumlah Pengguna Internet 2017 Meningkat, Kominfo Terus Lakukan Percepatan Pembangunan Broadband* (Jakarta: The Ministry of Communication and Information Technology, 19 February 2018).

⁷⁶ Fatimah Kartini Bohang, “Berapa Jumlah Pengguna Internet Indonesia?” *Kompas*, 22 February 2018, accessed 6 November 2018, <https://tekno.kompas.com/read/2018/02/22/16453177/berapa-jumlah-pengguna-internet-indonesia>.

Teenagers, aged 13 to 18 years dwell in the third position with a 16.68 percent..⁷⁷ Finally, only 4.24 percent of parents over 54 use the internet..⁷⁸ These numbers describe the enormous variety of people whose lives depend on cyber technology in diverse ways and various domains.

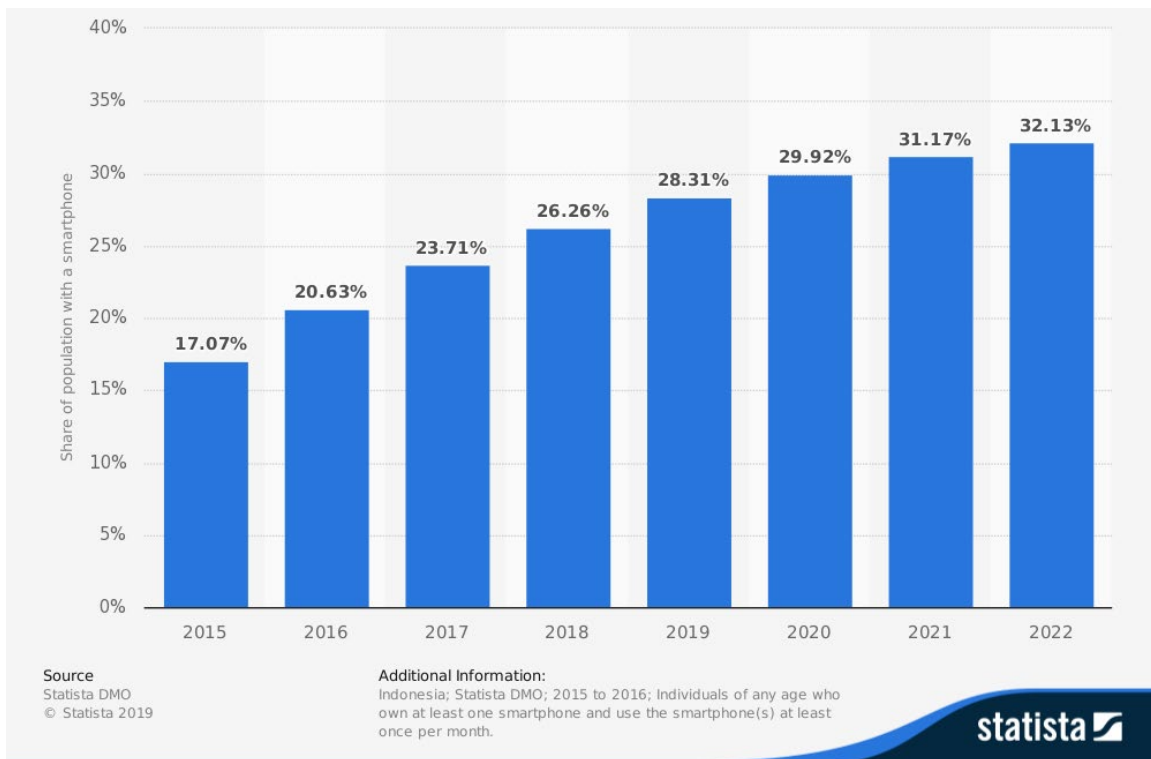


Figure 8. Smartphone Penetration Rate as Share of the Population in Indonesia (2015-2022)

Source: Statista, “Smartphone Penetration Rate as Share of the Population in Indonesia from 2015 to 2022,” Hamburg, Germany, 2019.

⁷⁷ Ibid.

⁷⁸ Ibid.

Overall, Indonesia has redesigned its economy toward high-value industry. Indonesia has been enhancing its economic value by utilizing the Information, and Communication Technology (ICT) industry, to include Mobile Internet, Cloud technology, Internet of Things (IoT), Big data, and advanced analytics in supporting its economic interest. Cyber technology provides Indonesia significant advantages for national defense and security also economic growth.

Nevertheless, all above is not a straightforward exertion because there are abundant of consideration to achieve those goals. The thriving of the digital economy comes with many challenges for nations. As new startups increase, and the digital economy industry boosts its productivity, there is an increased apprehension among technology professionals and scholars. One, and the foremost, are the cyber threats.

Dilemmas Caused by the Outrages of Cyber Threats and Risks

Despite its significant benefits, cyberspace can become a self-inflicted weapon that will harm the users. It can be easily hacked, operated, and arranged by intruders for their interests. Cyber-attack's less-boundary characteristic makes it difficult be identified and creates dubious environment to protect it. Indonesia has also suffered millions of cyberspace's double edge consequences. Cyberspace has been threatening national interests in many countries with various type of actors nationally or internationally.

Cyberspace threats have been alarming international community. In early 2018, the US Intelligence Community reported the global threat assessments asserting that cyber threat is the primary concern of global threat. This report predicts the unexpected-

boom of risks in the following years disrupting billions of digital devices connected..⁷⁹

Nations have experienced thousands of cyber-attacks encompassing hacktivism, corporate, espionage, government, driven, terrorism, and criminal which target value assets, reputations and other values based on their interest. The World Economic Forum 2015 portrays the cyber threats and risks as a figure below.

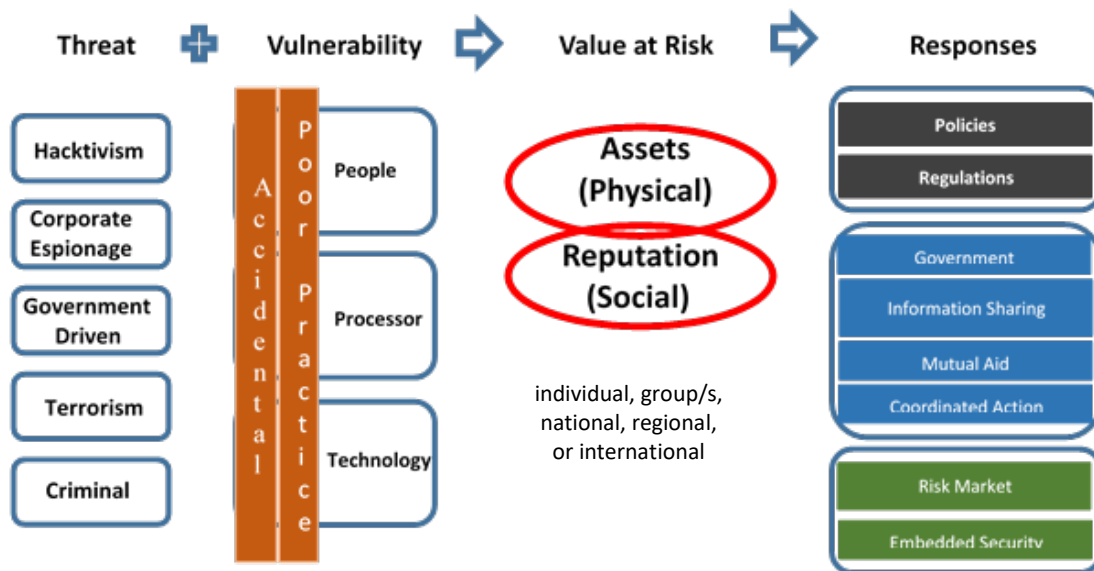


Figure 9. Cyber Risk and Responses Framework

Source: World Economic Forum (2015), quoted in Klaus Schwab and Nicolas Davis, *Shaping the Future of the Fourth Industrial Revolution, 2018* (Geneva, Switzerland: World Economic Forum, 2018).

⁷⁹ Daniel R. Coats, *World Wide Threat Assessment of the US Intelligence Community*, Statement for the Record (Washington, DC: Director of National Intelligence, 13 February 2018), 5, accessed 25 January 2018, <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.

Personal or various types of criminal groups can drive cyber-attack. Their intention might vary depending on resources available, vulnerability of target, and opportunity. Most of cyberspace felonious actions are still being committed by non-state actors for engender amount of profits by illegal deeds through trivial risks of being arrested.⁸⁰ During 2016–17 period, The Australian Strategic Policy Institute (ASPI) argued that no major threats on critical national infrastructure meaning that nation interests were not involved in deliberately reckless activities during the reporting period. The United States Office of Personnel Management (OPM) experienced data breached targeting the records of about four million people.⁸¹ Brian Krebs, an American correspondent and investigative journalist, believes that he successfully identified an alien country man behind one of the huge black-market sites that sell victim' personal data information for hundred US dollar per part.⁸² Another example happened in Singapore. The Singapore health care's report emphasizes the most serious data breach of 1.5 million patients' records including the Prime Minister.⁸³ These patient's data

⁸⁰ The Australia Strategic Policy Institute, *Cyber Maturity in The Asia–Pacific Region 2017*, 6.

⁸¹ Devlin Barrett, Danny Yadron and Damian Paletta, "U.S. Suspects Hackers in China Breached about 4 Million People's Records, Officials Say," *Wall Street Journal*, 5 June 2015, accessed 19 April 2019, <https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888>.

⁸² Nicole Perlroth, "Who Is Selling Target's Data?" *The New York Times*, 24 December 2013, accessed 19 April 2019, https://bits.blogs.nytimes.com/2013/12/24/who-is-selling-targets-data/?_r=0.

⁸³ Jessica Davis, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's," *HealthcareITNews*, 20 July 2018, accessed 24 January

breached of specialist clinics, and polyclinics between the middle of 2015 and 2018 might end up being sold.⁸⁴ Likewise, U.K. National Health's hospitals incident indicates the same experience with the condition of their magnetic resonance imaging (MRI) technologies, and other tools were unexpectedly unworkable that potentially bring the death of blameless citizens.⁸⁵

The Internet Security Threat Report (ISTR) 2017 testifies that the government and critical infrastructure organizations are vulnerable being targeted by worldwide variety of cyber-attacks.⁸⁶ Therefore the government's ability to recognize and categorize attacks is crucial in assessing which assets may be besieged and what elements can be appointed to mitigate that threats and risks. The report highlights several national level components that being vulnerable for being attacked such as the government, health systems, financial services, transportation, telecommunications, utilities, and manufacturing.⁸⁷ That reports assumes that attacks which targeting government agencies and organizations can be as a

2019, <https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers>.

⁸⁴ Eileen Yu, "Singapore Suffers 'Most Serious' Data Breach, Affecting 1.5M Healthcare Patients Including Prime Minister," Zdnet, 20 July 2018, accessed 26 January 2019, <https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/>.

⁸⁵ Ray A Rothrock, *Digital Resilience* (New York: American Management Association, 2018), vi.

⁸⁶ Symantec, *Internet Security Threat Report (ISTR) Government*, November 2017, 104, accessed 27 April 2019, <https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf>.

⁸⁷ Ibid.

mean of expressing political disagreement regarding policies or other types of interests. First, the actions may include blocking access of the government system, accessing restricted information by espionage, and discrediting the government to gain social impacts. These actions may affect disruption of national assets, revelation of the highly classified-information, and social concerns to create instability of national environments. Second, these actions may impact personal or individual threats. By stealing the governments information systems which store considerable quantities of personally identifiable information (PII) the actors can gain benefits and the individuals that being targeted become vulnerable. Consequently, the government information lost and disrupted could impact political instability, critical infrastructures suspended, and intelligence exposures.

Therefore, being executed by personal or various of group; however, the impact of cyber-attack can be significant depending on their motivation and intend. The cost of losing data, spying, and other criminal acts can simultaneously affect harmful consequences for personal, community, government agency, and even a nation, because simply in a very low level, for example, the hackers can steal names, government-issued identification numbers, addresses, bank accounts, and other potential data. If the hackers are recruited by the criminal groups or terrorist syndicates, they can provide bigger impact depending on personal capability, assets provided, and number of people that enable their achievement. It can be executed willingly or unwillingly as many shown by detective movies or documenter films. Indeed, if a country or nation as the actor - having a huge number of resources in term of human capitals, facilities, authorities, budget and other requirements – the impact will be incredibly huge. Other resources cover other

instance level of losses. The WannaCry manifest a new generation of cyber-attack in swiftness and scales, affected billions of dollars of global business, and infected 230,000 computer technologies around 150 countries.⁸⁸ The Stuxnet spoiled nearly twenty percent of Iran's nuclear plant and also affected Indonesia, India, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland, and Germany.⁸⁹ The "worm virus" infected more than one-fifth of a million processors and instigated substantially damaged a thousand machines in Iran.⁹⁰ The personal or group actors and targets vary depending on their purposes and type attack whether. Furthermore, the process of attack can be caused by the accidental or poor practice of the users, flawed processors, or low quality of technology.

⁸⁸ Tara Seals, "One Year After WannaCry: A Fundamentally Changed Threat Landscape," *Threat Post*, 17 May 2018, accessed 26 January 2019, <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/>.

⁸⁹ James P. Farwell and Rafal Rohozinski, *Stuxnet and the Future of Cyber War* (London, UK: Routledge, 2011), 23; Michael B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, 20 November 2013, accessed 1 August 2018, <https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>.

⁹⁰ Tim Ricketts, "Sheep Dip Your Removable Storage Devices to Reduce The Threat of Cyber Attacks," M.A.C Solution, 2019, accessed 12 April 2019, <https://www.mac-solutions.net/en/news/129-sheep-dip-your-removable-storage-devices-to-reduce-the-threat-of-cyber-attacks>.

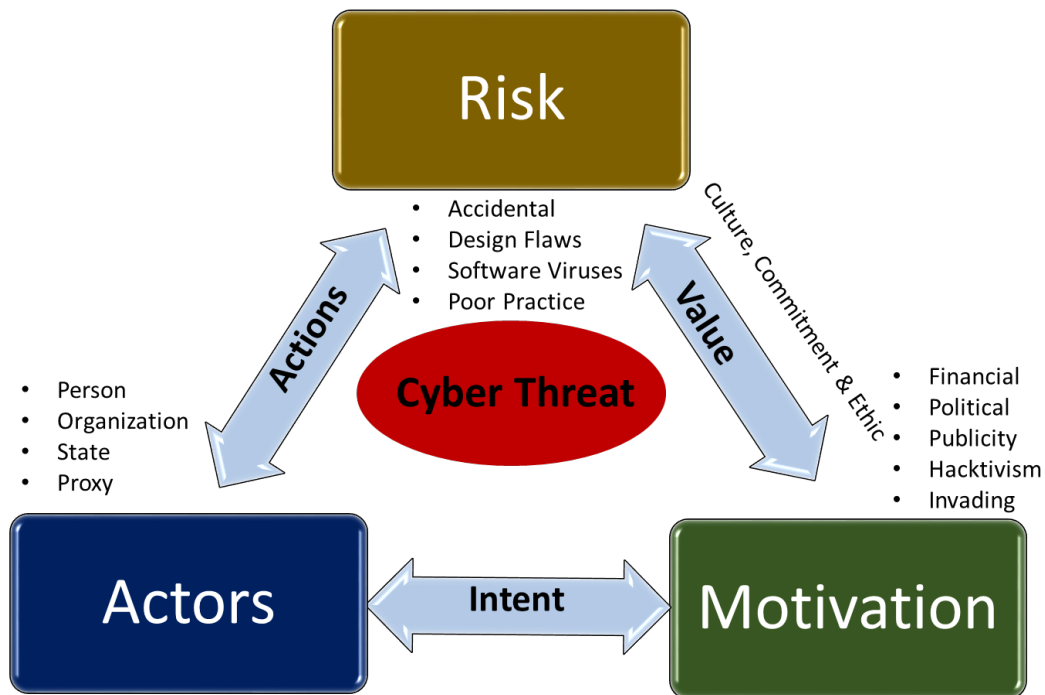


Figure 10. Cyber Threat Diagram

Source: Created by author.

Nevertheless, there have been some studies asserting their curiosity of national interest engrossment in cyber-attack. The Australian Strategic Policy Institute (ASPI) 2017 report emphasizes the national political and strategic effect of cyber threat highlighting Russia's alleged interference in the US election and North Korea's considerable monetary cyber threat that possibly affected its political power in that region.⁹¹ In 2016 and 2017, cyber malware attacked against Ukraine and Saudi Arabia

⁹¹ Alex Hern, "North Korea is A Bigger Cyber-Attack Threat Than Russia, Says Expert," *The Guardian*, 26 February 2018, accessed 10 January 2019, <https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia>.

targeting a number of critical infrastructures, government, and commercial networks that potentially target others.⁹² While in April 2010, the global world was shocked by WikiLeaks' disclosures publishing millions of classified and sensitive military and diplomatic documents.⁹³ In 2007, Estonia experienced an upsurge of hostile cyber-attacks that struck all of the country's Internet infrastructures, ranging from government sites and banking to local newspaper sites.⁹⁴ The two-week attack was able to paralyze the government of Estonia. Likewise, the same incident happened in 2008 causing the Georgian government's capabilities and its society disrupted.⁹⁵ Both nation or states and other types of malign actors became more heartened and well-resourced in wide-spreading cyber threats.⁹⁶

The global trend of disruptions and the rapid change of ICT or IoT has shifted the ways and means to protect state sovereignty. A nation's residents' affairs, nation's territory, and the government's policy, which is part of the sovereignty of the county, become more vulnerable. State boundaries do not limit cyberspace capability. Cyber

⁹² Symantec, *Internet Security Threat Report (ISTR) Government*, 8.

⁹³ Ibid., 153.

⁹⁴ Robert Coalson, "Behind the Estonia Cyberattacks," *RadioFreeEurope RadioLiberty*, 6 March 2009, accessed 1 August 2018, https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.

⁹⁵ Jim Nichol, *Russia-Georgia Conflict in August 2008: Context and implications for U.S. Interest*, CSR Report to Congress (Washington, DC: Congressional Research Service, 3 March 2009), accessed 2 December 2018, <https://fas.org/sgp/crs/row/RL34618.pdf>.

⁹⁶ Coats, *World Wide Threat Assessment of the US Intelligence Community*, 5.

actions take place on a region and involve objects, or are conducted by individuals or entities, over which states may exercise their sovereign prerogatives.⁹⁷ Experts noted that “although cyber activities may cross multiple borders, or take place in international waters, international airspace, or outer space, all are conducted by individuals or entities subject to the jurisdiction of one or more states.”⁹⁸ The continuation of policy by other means becomes more complex and dubious.

Having observed the dreadful impact of cyber-attacks, therefore, there are potential situations that can lead to cyberwar,⁹⁹ or cyberwar has been already happening, depending on how cyberwar terminology is being interpreted. The character of war has transformed since the improvement of technology.¹⁰⁰ Conflict and confrontation seem a part of human nature that has existed since the very beginning of society, and its nature is always changing, like the chameleon.¹⁰¹ Professor Martin Van Creveld defines traditional war as a clear approach for who instructs and pays; who struggles and dies;

⁹⁷ Michael N. Schmitt, *Tallinn Manual on The International Law Applicable to Cyber-Warfare* (New York: Cambridge University Press, 2013).

⁹⁸ Ibid.

⁹⁹ David Gewirtz, “Why The Next World War Will Be A Cyberwar First, And A Shooting War Second,” *ZD Net Government*, 22 June 2015, accessed 7 November 2018, <https://www.zdnet.com/article/the-next-world-war-will-be-a-cyberwar-first-and-a-shooting-war-a-distant-second/>.

¹⁰⁰ Ibid.

¹⁰¹ Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984).

who wages it; and who suffers,¹⁰² while in cyberwar, it is unclear and unexpected. If, in conventional warfare, actors need to conquer territory with boots on the ground to achieve their objectives, the cyberwar troops simply use their keyboards to defeat other nations. In the cyberspace, actors merely besiege the computer network system that is connected to countries' critical infrastructure to achieve their goals. The actors simply attack through computer systems affecting certain expected destruction or dysfunction of certain political or national security systems.¹⁰³ Tuuli Aug, an author of *Eesti Paevaleht*, describes the situation like feeling under attacking of an invisible enemy; frightening and uncontrollable. Aug states, "You suddenly could not get information; you could not do your job. You could not reach the bank; you could not check the bus schedule anymore. It was just confusing and frightening, but we did not realize it was a war because nobody had seen anything like that before."¹⁰⁴ Cyberwar is also inexpensive; its weapons are often designated through nations' victims computer systems that were targeted.¹⁰⁵

¹⁰² Martin Van Creveld, "Transformation of War Strategy in the 21st Century" (interview by Christina Schori Liang, Geneva Centre for Security Policy, 12 March 2018), accessed 12 September 2018, <https://www.gcsp.ch/global-insight/transformation-war-strategy-21st-century>.

¹⁰³ Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," Yale Law School Faculty Scholarship, 2012, 823, accessed 21 April 2019, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4844&context=fss_papers.

¹⁰⁴ Valentinas Mite, "Estonia: Attacks Seen as First Case Of Cyberwar," *RadioFreeEuropeRadioLiberty*, 30 May 2007, accessed 13 December 2018, <https://www.rferl.org/a/1076805.html>.

¹⁰⁵ Gewirtz, "Why The Next World War Will Be A Cyberwar First, And A Shooting War Second."

Minimal personnel are at risk, being wounded and killed, and victims are often unaware they are attacked and may never know the attackers.¹⁰⁶ The attackers can win the war without military actions as described by the Sun-Tzu's strategic war philosophy. The world is under constant attack from cyber threats.

Indonesia is not excluded from the global cyber threats because cyberspace is a boundary-less world. In 2016, The Malware Infection Index, by Microsoft, exposed that Indonesia was the second highest country in the Asia Pacific Region encountering malware threats.¹⁰⁷ Pakistan was the highest, followed by Indonesia. Bangladesh, Nepal, and Vietnam are respective countries after Indonesia. This research asserts that the Asia Pacific region was considered as the most vulnerable menace of malware risks. The Microsoft malware protection system, Windows Defender Advanced Threat Hunting team testified that groups of cybercriminals had been aggressively targeting governmental institutions including defense and intelligence agencies, as well as telecommunication providers in the South and Southeast Asia region since 2009.¹⁰⁸ That team stated, computer systems in those countries, particularly Indonesia, experienced

¹⁰⁶ Ibid.

¹⁰⁷ Microsoft Asia News Center, Malware Infection Index 2016 Highlights Key Threats Undermining Cybersecurity in Asia Pacific: Microsoft Report, Microsoft, 7 June 2016), accessed 21 April 2019, <https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/>.

¹⁰⁸ Ibid.

almost forty percent of malware attacks while the worldwide average was about twenty percent.¹⁰⁹

The Bank of Indonesia claimed that it suffered a 66.7 percent increase in malware attacks compared to 2014.¹¹⁰ In 2015, the Minister for Political, Legal and Security Affairs of the Republic of Indonesia asserted that the number of cyber-attacks increased by about 33% from 2014.¹¹¹ The Directorate General for Postal and Information Technology Affairs reported that in the period from January to mid-December 2014, the total attack data recorded by its monitoring system reached 48.4 million.¹¹² The Indonesia Security Incident Response Team on the Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) testified that Indonesia experienced around 42 thousand attacks per day.¹¹³ It is reported in an open source media that total of all malware activity detected, 37.72 percent was related to Disk Operating System (DOS) attacks, 20.93 percent were exploits, 18 percent trojans, 15 percent were unscrupulous undetected.¹¹⁴

¹⁰⁹ Ibid.

¹¹⁰ Faizin Ridho, Anton Yudhana, and Imam Riadi, “Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Denial of Service (DDoS) Secara Real Time” (Annual Research Seminar, Ahmad Dahlan University, Yogyakarta, Indonesia, 6 December 2016), 111.

¹¹¹ Ibid.

¹¹² Directorate General for Postal and Information Technology Affairs, *Annual Report 2014*.

¹¹³ Id/SIRTI-CC, *Pasukan Cyber Indonesia Harus Dipimpin Presiden!*

¹¹⁴ Agustinus Mario Damar, “Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017,” *Liputan6*, 22 December 2017, accessed 6 November 2018,

Besides being vulnerable to be attacked, Indonesia is also assessed as the source of cyber threats portrayed in Figure 11. During the period of 2016-17, ASPI indicates the enhancement of cyber maturity of nations in the Asia-Pacific region; by stating no major cyber-attacks happened during that period; that means very low indication that cyber threats in this region derive from of national actors' involvement or is government driven. More importantly, cyber-attacks in this region have been conducted by individuals or groups of people based on interests. Symantec, an American software company, in its Internet Security Threat Report (ISTR) 2016 asserts that Indonesia is the forth country on earth as the sources of origin for government-targeted attacks at 0.7 percent of global sources activity, which is led by the United States (90.4 percent), India (5.0 percent), and China (1.5 percent). The rest of the big ten are Brazil, Poland, Italy, South Africa, United Kingdom, and Singapore. However, Indonesia is absent from the top ten countries where attacks on the Symantec IoT honeypot were initiated which is led by China at 26.5 percent, followed by 17.7 percent in the United States, Russia Federation at 5.8 percent; less significantly are Germany, Vietnam, Netherlands, Ukraine, France, Japan, and United Kingdom.¹¹⁵ These conditions of the local threats, indeed, require respective governments to build international cooperation and coordination through developing cyber diplomacy in enhancing awareness, building cyber resilience capacity, creating a robust security system, and developing a strong interoperability system to mitigate that; in this writing, particularly in Indonesia.

<https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017>.

¹¹⁵ Symantec, *Internet Security Threat Report (ISTR) Government*, 103.

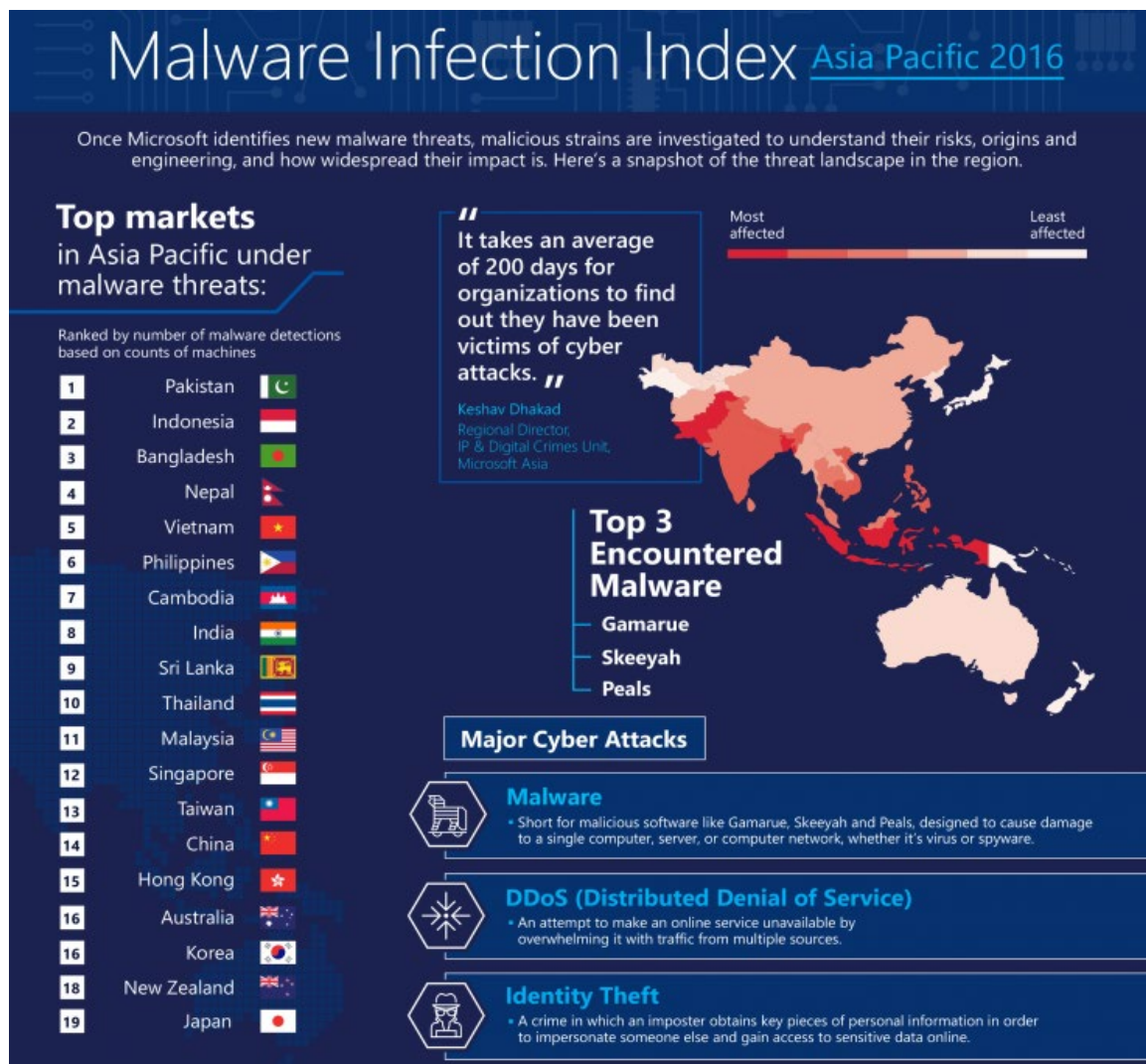


Figure 11. Asia Pacific 2016 Malware Infection Index

Source: Microsoft Asia News Center, “Malware Infection Index 2016 Highlights Key Threats Undermining Cybersecurity in Asia Pacific: Microsoft Report,” Microsoft, 7 June 2016, accessed 21 April 2019, <https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/>.

No country on earth feels immune to cyber-attacks; cyber threats happen everywhere on Earth. The more advance reliance of ICT technology, the greater concerns

of it, associated with risks and threats. Regardless of cyber threat sources, many countries have suffered. The government has been creating multiple efforts to mitigate the risks of double-edges of cyberspace' consequence. A history reminder, the capability of confronting threats is the primary objective in the Indonesia National Defense Strategy. The ability of a nation to protect its internal values from external threats is significant to secure a nation.¹¹⁶ Indonesia achieved independence in 1945 from colonialism and was tested twice by foreign military aggression in 1947 and 1948, as well as domestic security threats from separatism and radicalism.¹¹⁷ In 1990, Charles S. Maier, Professor of History at Harvard University, mentions how significant it is for a nation to have the capacity to control its domestic or/and foreign conditions to provide prosperity and well-being for that nation.¹¹⁸ Consequently, Indonesia also needs to consider these new forms of threats to be mitigated. As part of international community, there are some aspects that Indonesia can observe from that international exertions.

Lessons Learned from International's Approaches in Achieving Cyber Resilience Capacity

To cause ICT's roles to run more effectively and being capable to mitigate cyber threat, it is necessary for Indonesia to have additional references from the international

¹¹⁶ Romm, *Defining National Security*, 5.

¹¹⁷ Louis Zweers, *Agressi II: Operatie Kraai. De Vergeten Beelden Van De Tweede Politionele Actie* (Netherland: SDU Uitgevers, 1995); Raditya N. Iswara "Agresi Militer I: Saat Belanda Mengingkari Perjanjian Linggarjati," *Tirto.id*, 21 Juli 2018, accessed 15 January 2019, <https://tirto.id/agresi-militer-i-saat-belanda-mengingkari-perjanjian-linggarjati-cs8T> 21 Juli 1947.

¹¹⁸ Charles S. Maier, *Once Within Borders Territories of Power, Wealth, and Belonging since 1500* (Boston, MA: Harvard University Press, October 2016), 215-335.

community. Cyber diplomacy and international cooperation have been facilitating this effort providing Indonesia a shared-knowledge and experience from other countries to enhance its cyber resilience capacities. Those lessons learned can be achieved from several international forums and organizations which provide assessment for enhancing cyber resilience capacity.

The world has been developing cyber resilience capacity to encounter the threats in the cyberspace. Cyber resilience seems to be new terminology with minimal discussion compared to cyber-security, cyber-defense, and cyber-crime. However, in the World Economic Forum annual meeting in Davos, 2011, world leaders and experts discussed establishing a project to build cooperation for increased cyber resilience. Furthermore, in the World Economic Forum Report, 2016, the participants argued that “cyber resilience is more than just about cybersecurity. It incorporates business practices and entails being able to absorb attacks, recover from them, and restore business operations as quickly as possible.”¹¹⁹ Cyber resilience concerns for thousands of random and stealthy attacks, which have been impacted by intruders, enabling them to quickly recover and re-operate. Thus, cyber resilience does not deny the existence of cyber threat, yet it provides a flexibility for a cyber system to re-utilize despite in indecent situation.

However, the process of achieving cyber resilience capacity, in supporting national efforts to achieve its objectives, may encounter significant challenges. The government has many branches, ministries, departments, and agencies that rely on the

¹¹⁹ Brianna Keys, Aashish Chhajer, Zilong Liu, and Daniel Horner, *A Framework for Assessing Cyber Resilience* (Geneva: World Economic Forum, 2016), accessed 13 February 2019, http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf.

ICTs' role. Thus, achieving unity of effort is the primary concern to be obtained just like a joint operation of Armed Forces that consists of several services and branches. Without a robust system of harmonization and synchronization of communication and sharing understanding of environment through intelligent collection among all units and elements, the military commanders would face difficulty to visualize their understanding and make decisions to win the battle. On the national level, within more complex chain of commands and structures, in spite of the same necessity of unity of effort, it would encounter similar issues that is known as interoperability interagency.

There is rudimentary instance of challenge to achieve a unity of effort or interoperability in a real situation. The World Economic Forum 2015, for example, asserts that an interoperability is the most challenging in achieving the cyber resilience capacity. By sampling some industrial cyber systems, World Economic Forum researches the essential barrier in industrial internet deployments. Although the samples derived from the forty-three industries from North America and thirty samples from Europe, this assessment can be a tool for referencing the global industries' cultures. Back to the national level, it facilitates a government to visualize the challenge of interagency interoperability among the related-agencies. Furthermore, the World Economic Forum adds that lack of interoperability will significantly increase complexity, ineffectiveness, and inefficiency in industrial – and as discussed earlier, in the national level – systems.¹²⁰

¹²⁰ Schwab and Davis, *Shaping the Future of the Fourth Industrial Revolution*, 106.

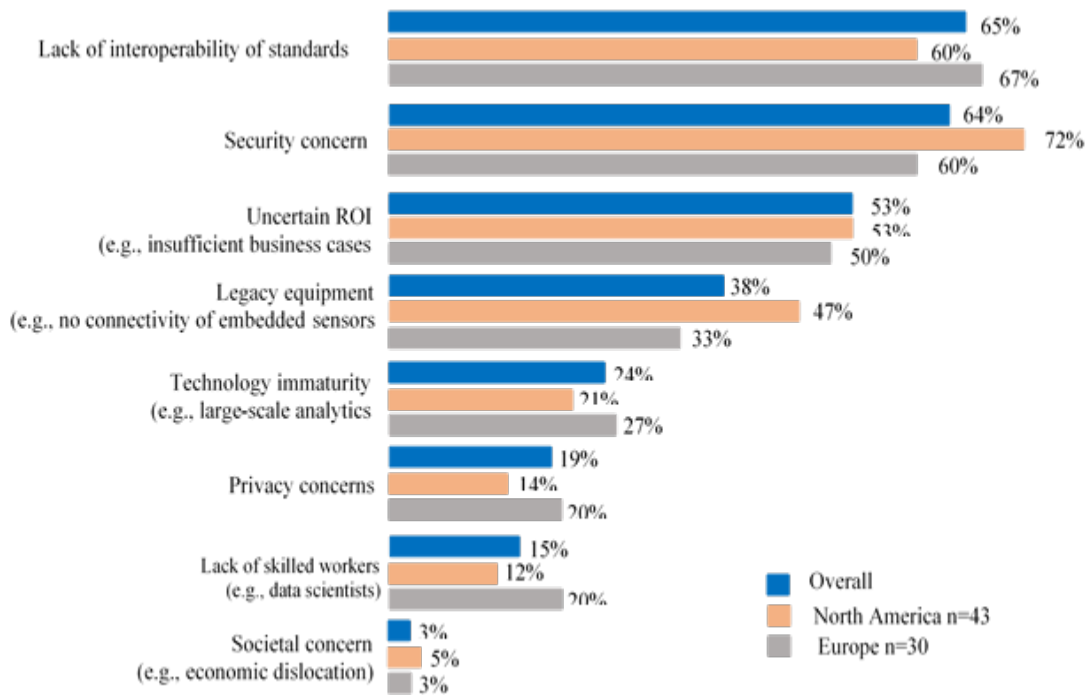


Figure 12. Key Barrier in Adopting the Industrial Internet

Source: World Economic Forum Survey (2014), quoted in Klaus Schwab and Nicolas Davis, *Shaping the Future of the Fourth Industrial Revolution* (Geneva, Switzerland: World Economic Forum, 2018), 107.

Figure 12 depicts the World Economic Forum 2014's discussion about how the industrial Internet of Things could unleash the potential of connected products and services. The forum highlighted that lack of interoperability and security concerns as the two utmost hurdles before the uncertain return on investments on current technologies, immature or untested technologies, and lack of data governance. In the future, wholly functional digital environments will require unified information sharing among technologies and other systems from different industries. Moreover, other prominent barriers and risks contain uncertain returns on investments on new technologies, immature or unapproved technologies, lack of data governance rules, and a lack of digital

aptitude. These challenges strongly require leadership, investment, and collaborative actions among key stakeholders or in the national level is interagency.¹²¹

Interagency as the most challenging to build a national unity of effort is also being described in The Global Cybersecurity Index (GCI) 2017. CGI 2017 is the last updated research conducted by ITU based on the survey throughout 2016 to promote a global culture of cybersecurity and its incorporation with the ICTs' core. Thus, GCI facilitates ITU Member States to develop cybersecurity and integrate it on a global scale of national activities by providing an assessment.¹²² Regarding to prior discussion, Indonesia needs to have a courtesy of that assessment portraying the lack of interagency interoperability in developing its cyber resilience capacity. That analysis is based on GCI 2017's observation and analysis of Indonesia cybersecurity development highlighting organizational and cooperation pillars including Indonesia's existing partnership systems, supportive agendas, and information sharing nets.¹²³ Both pillars are intercorrelated with expected interagency interoperability system in Indonesia. Literally, cooperation pillar has an interagency partnership dimension as the most noticeable aspect in it; however, there are other aspects enabling interoperability efforts including bilateral agreements, multilateral agreements, and international participation that link to cyber diplomacy and development technical capacity. There is one aspect that effects the effectiveness of interagency interoperability in GCI 2017 so called public-private partnerships; however,

¹²¹ Schwab and Davis, *Shaping the Future of the Fourth Industrial Revolution*, 107.

¹²² ITU, *Global Cybersecurity Index (GCI) 2017*.

¹²³ *Ibid.*, 4.

this aspect is not covered in this thesis. The organizational pillar provides strong points for enhancing interagency interoperability. It encompasses cybersecurity strategy, responsible agency, and cybersecurity metrics that are as essential as the strategic and operational guidance. However, based on Table 8, Indonesia was assessed in the “maturing stage (scored 50-89 percentile)” in responsible agency dimension; and, Indonesia was measured in the “initiating stage (scored lower than 50 percentile)” in strategy and cybersecurity metrics. Those indicators provide a visualization for the Indonesia government to tailor its interagency cooperation and relationship among the existing cyber agencies to achieve cyber resilience capacity.

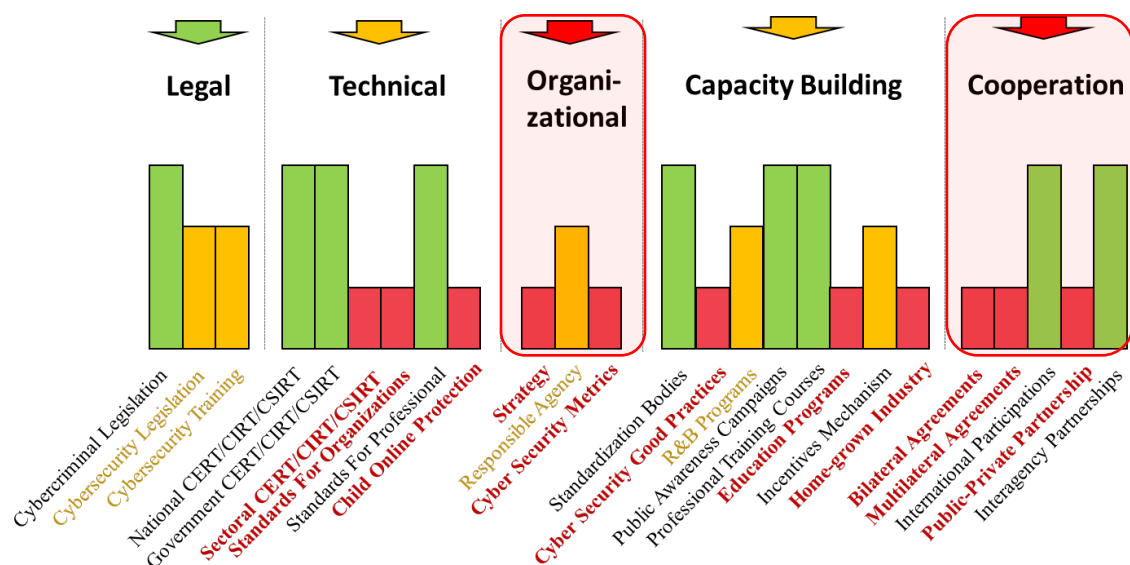


Figure 13. Indonesia GCI 2017 Indicator Assessments

Source: Created by author using data from The International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva, Switzerland: ITU, 2017).

Australian Strategic Policy Institutes (ASPI) 2017 also provides some views through its Cyber Maturity 2017. Initially, ASPI's function is to provide recommendations to the Australian Government regarding security, defense, and strategic policy issues. Internationally, ASPI has International Cyber Policy Centre expanding its role to facilitate cyber understanding, research, consultation with government, business, and civil society in the Asia Pacific Region. ASPI uses "cyber maturity metric" to contribute the assessment of twenty-five country participants encompassing South, North and Southeast Asia, the South Pacific, and North America.¹²⁴ Cyber Maturity 2017 describes the maturity of cyber development in the Asia Pacific region arguing that this region has successfully enhanced its cybersecurity management. In this region, Indonesia is surrounded by countries which have a clear roadmap of National Cyber Security Strategy (NCSS): Singapore 2016, Australia 2016, and National Cyber strategy of the United States 2018.

These countries consider the cyberspace as vital as securing air, land, and sea. Singapore launched its first cybersecurity master plan in 2005. The Cyber Security Agency of Singapore was created in 2015 as a dedicated entity to oversee cybersecurity, and the country issued a comprehensive strategy in 2016 signed by Prime Minister Lee Hsien Loong.¹²⁵ Australia started developing their cyber security strategy in 2009, and

¹²⁴ The Australian Strategic Policy Institute, *Cyber Maturity in The Asia-Pacific Region 2017*.

¹²⁵ The Ministry of Communication and Information of Singapore, *Singapore's Cybersecurity Strategy* (Singapore: CSA Singapore, 2016), accessed 15 November 2018, <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>.

the president of Australia signed to release its most updated cybersecurity strategy in April 2016.¹²⁶ The president of the United States put his signature on the National Cyber Strategy in September 2018. Like two others above, the United States' National Cyber Strategy describes the broad concept interoperability among the agencies to reach the national objectives in cyberspace. The United States administration is integrating cyber into all elements of national power by structuring the National Cyber Strategy to achieve the four pillars of the National Security Strategy (NSS).¹²⁷ Table 5 shows three countries' assessments followed by Indonesia's description based on GCI 2017 in developing their cybersecurity to achieve cyber resilience capacity.

Table 5. Two Most Committed Countries Based on GCI 2017 and Indonesia Position						
Country (Rank)	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore (1)	0.92	0.95	0.96	0.88	0.97	0.87
United States (2)	0.91	1	0.96	0.92	1	0.73
Australia (7)	0.82	0.94	0.96	0.86	0.94	0.44
Indonesia (70)	0.424	Not Mentioned				

Source: Created by author using data from The International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI) 2017* (Geneva, Switzerland: ITU, 2017 ITU, Global Cybersecurity Index (GCI) 2017), 17.

¹²⁶ Nicola Brangwin, *National Security—Cybersecurity* (Canberra: Commonwealth of Australia, 2016), accessed 15 November 2018, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/Cybersecurity.

¹²⁷ Grant Schneider, "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," The White House, 20 September 2018, accessed 13 December 2018, <https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years>.

Singapore is the top-ranked country in the Southeast Asia region. This island-state has a long history of cybersecurity initiatives and exceeds other countries in its CGI 2017 “cooperation pillar,” as listed in Table 5. Singapore exceeded the United States in total score, surpassing the United States’ perfect score in legal system and capacity building. Singapore achieves the utmost mark in cooperation with a score 0.87 when the United States is at 0.73. That CGI score makes Singapore achieve the highest readiness ICT system protection and resilience in the ASEAN region and even in the world based on their pillar assessment.

Table 6. The Most Matured Countries Based on Cyber Maturity in the Asia-Pacific Region 2017, Singapore and Indonesia Position						
Country (rank)	Total Score	Governance	Cyber-crime	Military	Business	Social
United States (1)	90.8	8.75	10	10	9	9
Australia (2)	88.0	8.75	9	8	9	9
Singapore (4)	87.7	8	8	9	10	9.5
Indonesia (12)	54.3	5.5	6	6	6	4

Source: Created by author using data from The Australia Strategic Policy Institute, *Cyber Maturity in the Asia-Pacific Region 2017* (Barton ACT, Australia: International Cyber Policy Centre, December 2017), 18-22, 39-41, 69-71, 84-87.

Moreover, Cyber Maturity 2017 considers Singapore for having a robust cyber interoperability after the United States and Australia among pacific countries. Singapore successfully integrates its government sector including military and law enforcement forces to enhance its national cyber resilience capacity as described in Table 6. Singapore has an almost perfect score in business and social pillar of the Cyber Maturity in The Asia-Pacific Region 2017. Singapore surpasses the United States and Australia with its

point at 10 and 9.5 respectively. The business pillar is assessed by quality/level of interaction between government and industry regarding cyber issues. This pillar also measures the level of digital economy engagement in contributing and enabling economic activity. Additionally, the social pillar considers the proportion of people accessing the internet, public awareness, and media coverage of cyber issues.

Having observed both GCI 2017 and the Cyber Maturity in The Asia–Pacific Region 2017, the United States was categorized in the most prominent position. The United States (0.92) excelled Singapore (0.88) in the organizational pillar in GCI 2017. Along with Australia, the United States achieved the highest score in the governance pillar of Cyber Maturity in The Asia–Pacific Region 2017 with score 8.7.¹²⁸ The government pillar in Cyber Maturity 2017 was assessed based on the effectiveness of implementation of the government’s organizational structures for cyber matters including policy makers, security, critical infrastructure protection, CERT, crime and intelligent, and consumer that integrated within Cybersecurity and Communication Center (NCCIS) as shown in Figure 14.¹²⁹ Besides the Cybersecurity and Communication Center (NCCIS), the United States developed the multilateral sharing agreement. The United States of America commenced cyber sharing and interoperability interagency agreement in 2015. The Multilateral Information Sharing Agreement (MISA) obligates government agencies from the department of defense, intelligence, justice, health, and energy to

¹²⁸ The Asia Pacific Policy Institute, *Cyber Maturity in The Asia–Pacific Region 2017*.

¹²⁹ Ibid.

enable each other in developing efficiency and effectiveness of cybersecurity information sharing to develop the Information Sharing Environment (ISE).¹³⁰

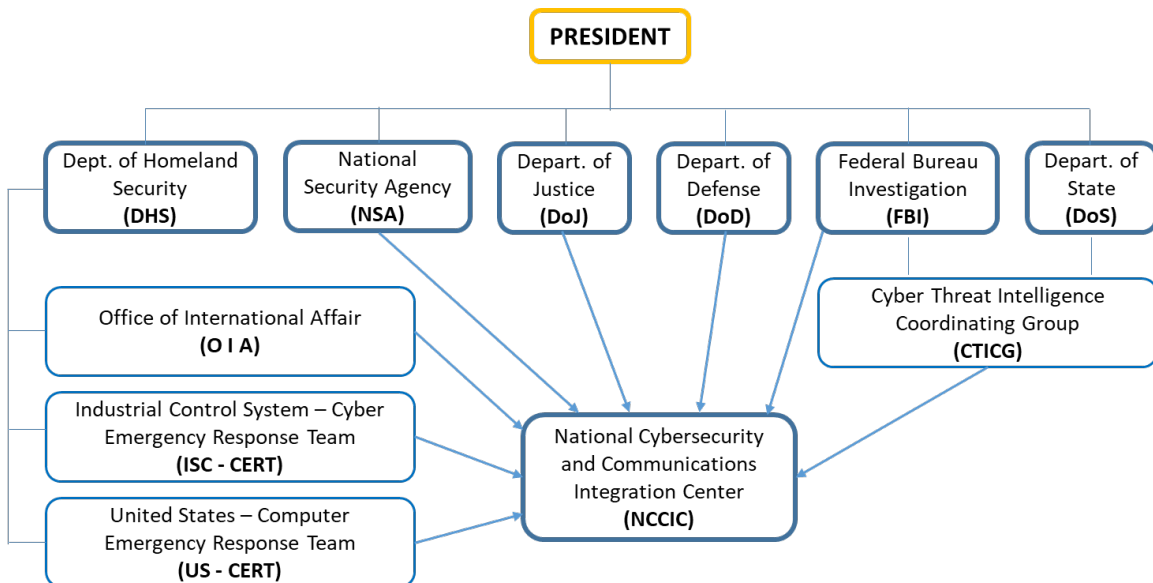


Figure 14. U.S. Cyber Coordination and Cooperation Model

Source: Created by author.

If individuals need to observe a deep example in one department, the United States Department of Defense established a military interoperability system known as the United States Cyber Command (USCYBERCOM). USCYBERCOM was established in August 2017 as one of the Unified Combatant Commands, and after several years it operated under the United States Strategic Command (USSTRATCOM). The purpose of USCYBERCOM is to plan, coordinate, integrate, synchronize, and conduct activities to

¹³⁰ Office of the Director of National Intelligence, “About the ISE,” 2018, accessed 24 January 2019, <https://www.ise.gov/blog/kshemendra-paul/coordinating-cybersecurity-programs>.

support its national interest from strategic to the tactical level – along with other Unified Combatant Commands which are the United States Special Operation Command (USSOCOM), the United States Strategic Command (USSTRATCOM), and the United States Transportation Command (USTRANSCOM). By this system, the United States expects a full-synchronized and harmonized cyber system throughout the US Military Armed Forces regardless of branches and services. This example provides a visualization of how significant an interoperability interagency can contribute success and systems enhancement.

The networking system in Figure 14 facilitates the United States to enhance its cyber resilience capacity. The networking system facilitates government agencies to share and synchronize situation and environment understanding to solve particular matters on the national level. The ICTs' core in the United States encompasses all aspects started from national security interests, economic prosperity, leadership, and political means. Those values depend on the interoperability, security, and resilience of cyberspace. The global nature of cyberspace demands robust international participation and collaboration to achieve its goals. Therefore, the U.S. government enhances cyberspace international cooperation to endorse its vision of interoperable, reliable, and secure national cyber domain to achieve national aims.

All in all, there are some remarkable analysis from the international organizations to enhance Indonesia cyber resilience capacity. First and foremost, interagency interoperability is the key factor. Next, a country is to have a National Cybersecurity Strategy to harmonize and synchronize cyberspace situational understanding among agencies to support decision makers to enable cyberspace in enhancing national security,

defense, and prosperity. Furthermore, the government is also required to acquire a National Cyber Agency as the national cyber center or government's main effort and possess a networking system to achieve interagency unity of effort and those objectives.

The Establishment of Indonesia National Cyber Security Strategy

The first—and most important—area that indicates a country's cyber readiness is the articulation and publication of a National Cyber Security Strategy that aligns the country's economic vision with its national security imperatives.

— Melissa Hathaway, *Potomac Institute for Policy Studies Cyber Readiness Index 2.0 A Plan for Cyber Readiness: A Baseline and an Index*

A National Cyber Security Strategy is the primary prerequisite for a country to enhance its national cyber resilience environment. The Indonesia government, in June 2017, pronounced the establishment of a national cybersecurity strategy with its strategic vision, which is to integrate all national elements to participate in enhancing cyber resilience capacity encompassing government, cyber industry, scholars, and cyber community.¹³¹ The National Cyber Security Strategy that chains Indonesia's economic vision with its national security imperatives is the first—and the absolute prerequisite that indicates Indonesia's cyber resilience.¹³² The government is the primary means in achieving the National Cyber Security Strategy's goals.

¹³¹ BSSN, *Strategi Keamanan Siber Nasional*.

¹³² Hathaway et al., *Cyber Readiness Index 2.0 A Plan for Cyber Readiness: A Baseline and an Index*.

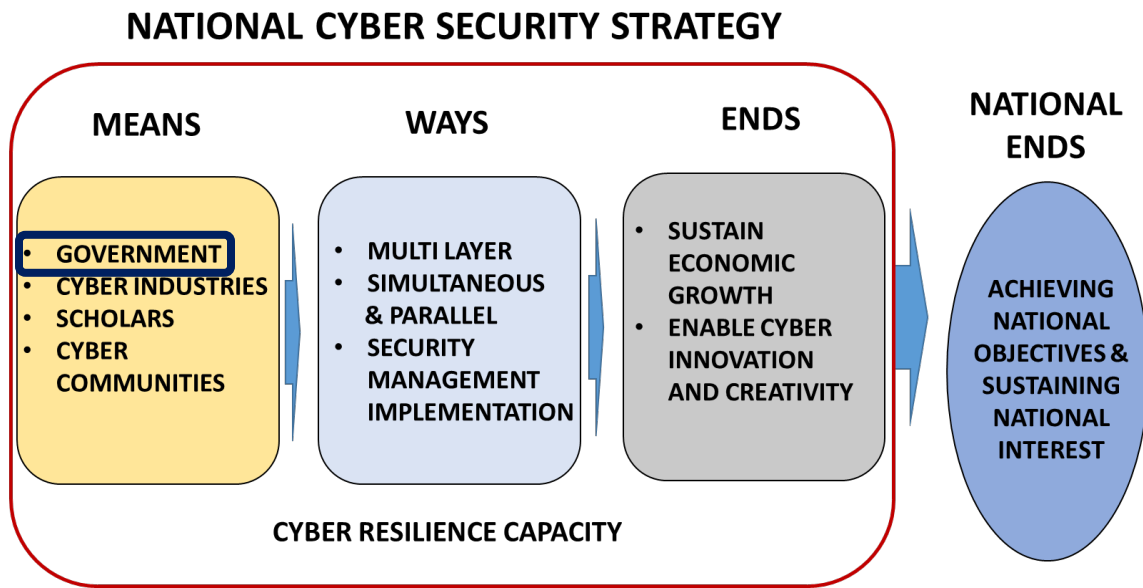


Figure 15. National Cyber Security Strategy Framework

Source: Created by author.

The government's roles and its cyber development planning are fundamental to mitigate cyber threats and risks. The National Cyber Security Strategy highlights five government roles in achieving those objectives. First, the Indonesian government is to protect the national cyber environment to allow freedom of connections across the country and have the public's software services sustained by international sharing of ICT. Second, the government is to protect the national e-Commerce system which is the backbone of Indonesia's digital economic growth. By promoting E-commerce, the Indonesian government expects economic revenue of ten billion USD by 2021 under coordination of the Ministry of Communication and Information Technology. Third, the government is to protect national critical information infrastructures that encompass government affairs, defense and security aspects, banking and national finance system,

health, energy and mineral resources, transportation, ICT, and food security. Currently, Indonesia has been developing national critical infrastructure outside Java – altering from Java centric development - which requires enormous ICT technology and national budget. The Indonesia government has built several seaports, airports, and main roads to enhance tourism infrastructures. Indonesia has enthusiastically been improving the quality of human resources by developing education technology, increasing food security, and health. For achieving those, Indonesia creates a conducive investment atmosphere to promoting clean government with its effective and efficient services. Regarding food security, Indonesia has been attempting to decrease exports of raw/unprocessed commodities, which means that Indonesia needs to increase its industrial system to support its productivity process, develop SME businesses, provide incentives, and increase logistic connectivity reaching rural areas. This process mostly requires ICT technology that requests to be protected. Moreover, the Indonesian Government has a role to control penetration in regard to ideology, politics, social concerns, cultures, and national defense and security as part of the protection of national objectives and interests.¹³³ Finally, the government has to protect Indonesian's citizen and their privacy which is one of the most concerns in daily life. As depicted on the Figure 1, Indonesia has considered amount of internet users reaching 92.5 million in 2018. These efforts are the primary concern of the government's role to reach Indonesia's resilience capacity by promoting the goals of the National Cybersecurity Strategy.

¹³³ BSSN, *Strategi Keamanan Siber Nasional*.

Furthermore, the National Cybersecurity Strategy underlines the development of cyber capability to enhance an expected level of capability in specific matters. This aspect consists of developing cyber intelligence, cyber defense, cybercrime, cyber diplomacy, and cyber economics which are interrelated with the Indonesia government's role in the National Cybersecurity Strategy as stated above.¹³⁴ The Indonesia government is required to enhance its cyber intelligence capability for detecting national threats which provides an early warning for defense and security approaches. Cyber defense and cybercrime are inter-correlated in terms of leveling the national threats. Cyber diplomacy facilitates the national cyber strategy to acquire diplomatic tools to discuss cyber risks and threats at regional and international levels. International partnership is crucial to develop cyber resilience capacity and protect nations against the common enemy so called cyber threats. Finally, cyber economy is the primary tool to promote Indonesia's growth, enhancing Indonesia's quality of lives in education, health and prosperity, and build national strong character as the independent country. Overall, those aspects will facilitate government decision makers to conduct actions, reactions, and counteraction to protect Indonesia and its society, promoting international relationships and upsurge Indonesia's growth in achieving national objectives and protecting national interests.

Based on analysis above, the government has been pursuing to utilize cyberspace technology in enhancing the national objective's achievement. The national development programs are part of government's effort to reach the national objectives. This current Indonesia administration defines the development program based on nine progress

¹³⁴ BSSN, *Strategi Keamanan Siber Nasional*.

priorities called “Nawa Cita.” – the development agendas translated into the 2015-2019 National Mid-term Development Plan.¹³⁵ These priorities encompass a primary aspect of protecting all citizens, developing truthful and effective government, develop peripheral areas, reforming law enforcement agency, improving quality life, increasing productivity and competitiveness, developing domestic strategic sectors, enhance character building, and strengthen spirit unity in the diversity of Indonesia. Indonesia has been promoting smart Indonesia, healthy Indonesia, and welfare of the marginalized group to improve the quality of life. Indonesia also has been targeting productivity and competitiveness improvement by enhancing national connectivity, urban transport, housing, infrastructure, investment, a state-owned enterprise, innovation, economic growth, trade, labor competitiveness, and economic data. Moreover, Indonesia determines seven aspects of strategic economic sectors: food, water, energy, natural resources, maritime, finance, and fiscal.

To boost efforts for Indonesia’s growth, the government highlights digital revolution through simplification of trades regulation, shifting services from paper-based to online approach. This alteration system is intended to create clean, effective, democratic, trustworthy governance agencies, and provide proficient quick-services. This is the second primary concern of the current official, after protecting Indonesian people and ensuring security for all citizens. The government has been fighting for corruption, inefficiency, long-bureaucracy process, and the unsynchronized national and provinces

¹³⁵ The United Nations Development Programme (UNDP) Indonesia Country Office, *Converging Development Agendas: ‘Nawacita,’ ‘RPJMN,’ and SGDs*, UNDP, November 2015), accessed 30 January 2019, <http://www.id.undp.org/content/dam/indonesia/2015/doc/publication/ConvFinal-En.pdf>.

regulations in some cases. Indonesia's approach to counter these issues is feasible and acceptable as shown in Figure 16 based on World Economic Forum's executive opinion that were asked to select the five most problematic factors for doing business in their country.

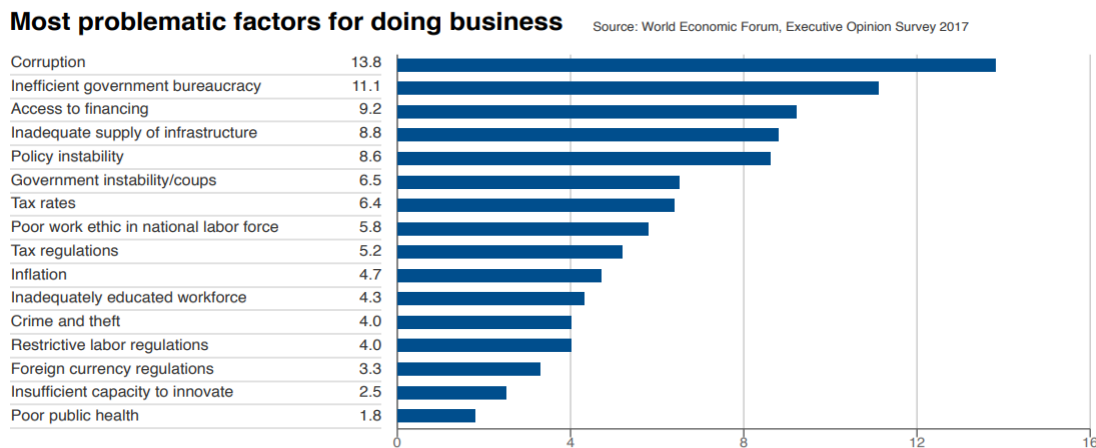


Figure 16. Most Problematic Factors for Doing Businesses

Source: International Monetary Fund, “World Economic Outlook Database,” April 2017, quoted in World Economic Forum, *Indonesia - The Global Competitiveness Index 2017-2018 Edition* (Geneva: World Economic Forum, 2017).

However, there is a trivial concern regarding the existence of Indonesia National Cyber Security Strategy. A year before the establishment of the current national cyber strategy by BSSN, in December 2016, the Indonesia Ministry of Communication and Information formulated a National Cybersecurity Strategy. There are some different objectives and priority areas that can impact the implementation of Indonesia strategy in cyberspace affairs.

The 2016 National Cyber Security Strategy consists of five key objectives and six priority areas.¹³⁶ It starts with the objectives by highlighting the cyber resilience role in supporting national critical information infrastructures. The purpose of this strategy is to ensure critical information infrastructure being resistant to cyber threats and capable of serving even if it is partially damaged by cyber-attacks. Then, it focuses on cyber public services, related to the establishment of response and recovery assistance through information sharing techniques, collaborations, and actions. It also underlines the objective to develop cyber law enforcement by the establishment of a framework of the enforcement of laws and regulations that can create safe and conducive cyberspace activities. Furthermore, it has objectives to build a cybersecurity culture through the creating common assessments of information security. Finally, this National Cyber Security Strategy highlights a cyber-secure market by the establishment of cyber competency and expertise along with cyber security capacities. These objectives are executed inside the area priorities of cyberspace including information security culture and capacities; risks; risk mitigations; incidents; management performances; and, law enforcement capacities in ICTs areas.

On the other hand, the 2017 National Cyber Security Strategy is divided by six key objectives and six priority areas. The primary objective is to increase national capacity and competitiveness for the economic growth and, the other five objectives are

¹³⁶ Aidil Chendramata, *Indonesia Cyber Security Strategy* (Jakarta: Directorate of Information Security, Ministry of Communication and Information Technology of Indonesia, 2016), accessed 17 January 2019, http://dephub.go.id/public/files/uploads/posts/posts/postbody/strategi_cs_nasional_desember2016.pdf.

related to cyber innovation and creativity. The National Cyber Security Strategy is to ensure security access of information and protect Indonesian Citizens and their personal data. Its purpose is to ensure the implementation of cyber standard security system in national agencies which is the most related to interoperability interagency and capacity building. It is to establish national cyber awareness and resilience capacity as well as the expectation of the establishment of the center for communication, cooperation, coordination, and collaboration on national cyberspace issues.

The 2017 National Cyber Security Strategy is implemented in six priority arenas. It includes national threats and challenges; contemporary cyber architecture; security and contingency management; international collaboration; invention and creativity; and, law enforcement. It identifies that there are two branches of national threats. First are the actual threats consisting of drug misuses, terrorism, natural disasters, cyber threats, corruption, and radicalism. Second are potential issues regarding global warming, environmental pollution, global pandemic, horizontal conflict, energy, and water scarcity. Another aspect is the 2017 National Cyber Security Strategy, which defines the cyber architecture consisting of the government, cyber industries, scholars, and cyber communities with respective roles. The main similarity between these two strategies is the Indonesia government performs significant roles in the 2017 National Cyber Security Agency including protecting national critical information infrastructures; echoed in the 2016 National Cyber Security Agency's main purpose.

The purpose for observing these two national cyber security strategies is not for an assessment. The purpose is to describe the existence of the National Cyber Security Strategy in Indonesia. Moreover, the updated National Cybersecurity Strategy (2017)

echoes the previous established cyber strategy. Nevertheless, the minor question would be inquired as to whether both National Cybersecurity Strategies exist simultaneously, or the most current negates the previous one. Understanding this concept will facilitate a decisive action for establishing a networking cyber coordination system to determine the agencies' role, task, and responsibility in that system.

To sum up, the National Cyber Security Strategy contributes significantly for achieving Indonesia's dream in cyberspace. It associates with the national effort in achieving national objectives, specifically in economic growth. It has been positively shifting Indonesia economic approaches to a digital economy that provides efficiency and effectiveness in many domains. Furthermore, it promotes clean government, facilitates a comfortable and quick service systems according to increased economic growth to achieve national objectives. Furthermore, the Indonesian government's roles in the National Cyber Security Strategy will significantly impact the achievement of those objectives.

These roles and tasks given by National Cyber Security Strategy to the Indonesian Government indeed are to be accomplished. It encompasses all domains that support Indonesian power including ideology, politics, economics, social concerns, culture, defense, and security. Furthermore, prior to the establishment of the National Cyber Security Strategy, Indonesia created the national cyber agency as the center of national cyberspace which is named the National Crypto and Cyber Agency.

The Indonesia National Crypto and Cyber Agency

Before the establishment of the National Cyber Security Strategy, to achieve the high level of cyber capacity, readiness and awareness, the Indonesia government created

a national cyber security agency known as the National Cyber and Crypto Agency (BSSN). The establishment of this agency is intended to be the National Security Center in achieving the National Cyber Security Strategy's objectives. BSSN is a Non-Ministry Government Institution that promotes national cyber awareness and cyber resilience capacity achievement.

Acknowledging the National Cyber and Crypto Agency

To deal with cybersecurity issues, we do not need to form a new institution or start from zero. We can expand or consolidate units at ministries or institutions that have cybersecurity functions.

—Widodo Joko, President of the Republic of Indonesia, *The Diplomat*

The National Cyber and Crypto Agency (BSSN) is an agency which is directly responsible to the President of the Republic of Indonesia. The President of Indonesia is assisted by several types of institutions under its administration: National Ministry, Non-Ministry Government Institutions, Non-Structural Institutions, Public Broadcasting Institution, and Structural Institutions Under National Ministries. BSSN is one of the twenty-seven Non-Ministry Government Institutions (LPNK) as a special agency that conducts specific tasks, cyberspace and cryptography. LPNK, formerly named the Non-Departmental Government Institution (LPND), is a state institution in Indonesia that was formed to carry out certain government tasks from the president. The head of the LPNK is under and is responsible directly to the president through a minister or minister-level official which coordinates it.¹³⁷

¹³⁷ The President of Republic of Indonesia, *The Law of the Republic of Indonesia Number 39 of 2008* (Jakarta: The Ministry of State Secretariat, 2008), ch. 6, art. 25, para. 2.

BSSN was created in 2017 through Presidential Regulation no. 53/2017 “about the establishment *Badan Sandi dan Siber Nasional* (BSSN). BSSN is an integration of National Crypto Agency, Directorate Information Security of the Ministry of Communication and Information Technology, and the Indonesia Security Incident Response Team on Internet Infrastructure coordination center (ID-Sirtii).¹³⁸ The National Crypto Agency was a national crypto central agency of the Republic of Indonesia, under the president, and is responsible to the president. It has been functioned to regulate, coordinate, and conduct protection for highly classified information among the national apparatus both at the national and regional levels. The Directorate Information Security was a directorate under the Directorate General of Information Application of Ministry of Communication and Information Technology. Furthermore, Indonesia Security Incident Response Team on the Internet and Infrastructure / Coordination Center (Id-SIRTII / CC) was appointed to oversee the security of internet protocol-based telecommunications networks under The Minister of Communication and Information. The idea of establishing Id-SIRTII / CC has begun to be delivered by several groups, especially practitioners, industries, academics, information technology communities, and the Government since 2005 before it was established in 2007. Id-SIRTII / CC has the main task of conducting socialization with related parties about IT security (information

¹³⁸ The Ministry of Communication and Information Technology of Republic of Indonesia, *BSSN Jadi Lembaga Utama Keamanan Siber* (Jakarta: Kominfo, 5 June 2017), accessed 8 November 2018, https://www.kominfo.go.id/content/detail/9800/bssn-jadi-lembaga-utama-keamanan-siber/0/sorotan_media; IGN Mantra, “Tumpang Tindih Tugas Badan Siber Dengan Lembaga Lain,” Detikinet, 8 January 2018, accessed 16 October 2018, <https://inet.detik.com/security/d-3805210/tumpang-tindih-tugas-badan-siber-dengan-lembaga-lain>.

system security), conducting early monitoring, early detection, early warning against threats to telecommunications networks from within and outside the country, especially in the act of securing network utilization, making / run / develop and log file databases and Internet security statistics in Indonesia. Thus, a transformation happened after the issuance of Presidential Regulation about BSSN. The National Crypto Agency becomes the main body, along with its employees being shifted into BSSN, likewise two other agencies. But, they are still fully operational in previous ministry or agency before BSSN is effectively fully-operated.

BSSN increases national cyber awareness and readiness. BSSN was created to achieve a strategic cyber environment to implement secure, interoperable, and reliable ICT systems. Besides promoting the digital economic growth, competitiveness, and innovation, BSSN is created to increase cyber awareness and national cyber resilience capacity. BSSN's core missions include preparations and actions in national cyber affairs..¹³⁹ It functions to conduct preparation enabling protection for electronic-based trading, coding, and screening at the national level. It is expected to be able to monitor and evaluate technical policies in various kinds of cyber activities regarding identification, detection, protection, and countermeasures. Therefore, BSSN is to be capable of providing recovery process, afford mitigation support for recovery of vulnerability situation of an incident and cyber-attack.

¹³⁹ Badan Siber dan Sandi Negara (BSSN), *The National Cyber and Crypto Agency Regulation Number 2 of 2018 concerning Organizations and Work Procedures for National Cyber and Crypto* (Jakarta: BSSN, 2018).

Cyber Maturity in the Asia Pacific Region 2017 report states that BSSN is expected to enhance Indonesia's official response to cyber threats and achieve cyber resilience capacity. Authored by ASPI, Cyber Maturity in the Asia Pacific Region 2017 highlighting Indonesia's improvement in cyber governance aspect. Indonesia's cyber governance aspect was graded five in 2016 to six point in 2017, stepping up maturity position of Indonesia cyber from fourteenth to twelfth in 2016, and remained the same in 2017 with two more country participants. BSSN is assessed for being capable in facilitating coordination and communication government agencies in enhancing the E-commerce system.

Furthermore, ASPI analyzed that Indonesia performs well in digital economy cyber awareness development. The highest score of Indonesia cyber maturity is its digital economics in supporting economic activity growth.¹⁴⁰ For examples, digital economics facilitate eight million digital small medium enterprises and a thousand striving digital start-ups. Indonesia enhances e-payment, e-commerce road map, enabling technology, logistics, cybersecurity, tax relief for tech companies, skills building, and consumer protection. The improvement of infrastructure can be observed by the industry logistics system, national bank activity and payment system, and other finance and statistics agencies of Indonesia. The upgrading efforts, however, also are followed by insufficient telecommunications infrastructure and lack of skills of the operators.

¹⁴⁰ BSSN, *The National Cyber and Crypto Agency Regulation Number 2 of 2018 concerning Organizations and Work Procedures for National Cyber and Crypto*.

Indonesia is also well assessed for its public accessibility in cybersecurity assistance service.¹⁴¹ ID-SIRTII/CC, along with its integration into BSSN, has contributed significantly in steering exercise and schooling on capacity building and research. Besides having participated in APCERT and FIRST, ID-SIRTII/CC also represents Indonesia's CERT communal at OIC-CERT, along with Cyber Security Malaysia (CSM), participating in the Organization of the Islamic Cooperation-Computer Emergency Response Team (OIC-CERT) part of twenty-one country member board.¹⁴² It systematizes the arrangement of denying hacker activities as a signature of the increase of cyber threat actor's skills.

To sum up, BSSN, as the new established cyber agency in Indonesia, is the fundamental tool for achieving national cyber resilience capacity. It will be a central to cyber agencies coordination in Indonesia and provides key approaches for the next action levels to achieve national unity of effort to reach the goal "national cyber resilience capacity." This expectation requires a deeper observation to achieve a comprehensive understanding to visualize ways and approaches to enhance this agency's capacity and capability.

¹⁴¹ BSSN, *The National Cyber and Crypto Agency Regulation Number 2 of 2018 concerning Organizations and Work Procedures for National Cyber and Crypto*.

¹⁴² Priyankar Bhunia, "Exclusive - Safeguarding Malaysian cyberspace (Part II) – International Cooperation, Changing Mindsets," Open Gov, accessed 6 February 2019, <https://www.opengovasia.com/exclusive-safeguarding-malaysian-cyber-space-part-ii-international-cooperation-changing-mindsets/>.

Potential Concerns and Solutions for BSSN to Implement the National Cyber Security Strategy

Cyber Maturity in the Asia Pacific Region 2017 asserts that Indonesia needs to enhance its interoperability, reliability, and security in cyberspace to tailor Indonesia's cyber resilience capacity and capability.¹⁴³ BSSN is the Indonesia government's primary means to enable and integrate the national unity of effort in cybersecurity strategy.

Overall, BSSN requires adequate time to become full operational; however, its establishment has been recognized by international cyber organizations. Nevertheless, BSSN potentially faces challenges in implementing the National Cyber Security Strategy's objective. The challenges might not be noticeable; however, it can impact the effectiveness of BSSN in succeeding its role. The new age of agency and the absence of networking coordination system can deter BSSN and the National Cyber Security Strategy to achieve its objectives.

Challenges as a New Transform Agency

BSSN, a new-aged government agency, consists of three different agencies. As mentioned earlier, the World Economic Forum asserts that interoperability is the most challenging for a new-built cyber industry, in this case, the new-aged of agency, BSSN. There has been studies that BSSN, just like other new organizations, would internally encounter challenges to building a cohesive team in shaping the organization's climate and culture to achieve the National Cyber Security Strategy's objectives.

¹⁴³ Bhunia, "Exclusive "Safeguarding Malaysian cyberspace (Part II) – International Cooperation, Changing Mindsets."

First, BSSN would face challenges to shape its internal organizational climate and culture which is one of the most problematic leadership challenges in a brief period. BSSN, an expected center of cyberspace agency in Indonesia, likely challenges this situation since it was formed by three distinct agencies that has firmly established and have their own climate and culture. Climate is a temporary condition, but it is a noticeable indicator of organizational culture. Thus, the leader's success to shape an organizational climate depicts the accomplishment of an organizational leadership. However, the success to shape a climate will be depending on the deep understanding of the existence of an organization's culture. Overcoming of resistance is the leader's principal challenge when facing a resistance for a transformation; thus, it is required to have a decent systems method for applying change within that organization. BSSN will be addressing an intertwining set of goals, characters, procedures, ethics, infrastructures performance, attitudes, and expectations issues from its assimilated agency.¹⁴⁴ A scholar's research asserts that, even after being established, a new agency may seem to make progress for a while, but in the end, the organizational culture's interlocking elements will take over and draw back to their firmed culture.¹⁴⁵ This is a the primary challenge for implementing the National Cybersecurity Strategy focusing on the government's roles coordinated by the new transformed-agency of national cyberspace center.

¹⁴⁴ Steve Denning, "How Do You Change an Organizational Culture?" *Forbes*, July 23, 2011, accessed 12 January 2019, <https://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/#6c60781839dc>.

¹⁴⁵ Ibid.

Furthermore, BSSN would encounter challenges regarding compliance and commitment of all organizations related to leveraging interoperability interagency. Adhering to the National Cyber Security Strategy's strategic vision, it is stated that the establishing and sustaining of national cybersecurity capability by synergizing stakeholders in participating in national security and increasing national economic growth is the primary prerequisite condition for achieving national cyber resilience capacity. The compliance can be caused by the availability of assets, existence of cyber operational units, capability building, and technical measure which are excluded from this writing. The objectives and functions coverage in the National Cyber Strategy encompass almost all national functions. The National Cybersecurity Strategy appears to create a total cyber protections system,¹⁴⁶ similar to Indonesian national defense principle that promotes the total people's war (*perang rakyat semesta*).

The unity of effort is the result of a strong commitment of organizations, but it would be one of the most concerns for BSSN. Observing day to day activities, most of commitment derives from compliance ranging from genuine compliance to noncompliance. Organizations that would genuinely enable Indonesia in achieving the National Cyber Security Strategy's objectives, by supporting BSSN, would be considered supportive while others that contribute the least amount of work are less-supportive. Yet, it is not the purpose of the establishment of a national cybersecurity center. Dr. Peter M. Senge, a Stanford and MIT alumnus and the leadership researcher, believes that commitment and capacity to learn at all levels is the fundamental aspect for a

¹⁴⁶ BSSN, *Strategi Keamanan Siber Nasional*, 6.

transformed-agency reaching a flexible, adaptive, and productive capability..¹⁴⁷ The true purpose is to build a unity of effort meaning every element contributes significantly for achieving the National Cybersecurity Strategy's objectives.

The establishment of national cyber security strategy opens the fundamental entry point for Indonesia for creating a robust national resilience capacity and capability. Its emergence depicts clear strategic guidance for the future cyber of Indonesia. However, Indonesia's national cyber strategy relies primarily on cyber interagency cooperation to achieve a comprehensive approach deal with the growth and expansion of cyber threats. The challenge is undisputable, that while determining roles and responsibilities inside its new-established agency, BSSN is to be able to predict national cyber capability and determine a potential solution to fill the gap of that capability.

Potential Solutions for the Implementation of Government's Approach in Achieving the National Cyber Security Strategy

The pressure on organizations to change will not only increase over the next decades. Yet the methods managers have used in the attempt to transform their companies into stronger competitors – total quality management, reengineering, right sizing, restructuring, cultural change, and turnarounds – routinely fall short, because fail to alter behavior.

— John P. Kotter. *Leading Change*

The World Economic Forum asserts that interoperability is the most prominent barrier in adopting internet industry which represents the challenges of agency cooperation system at national level. This challenge strongly requires leadership,

¹⁴⁷ Mark K. Smith, "Peter Senge and the Learning Organization," Infed, 2001, accessed 25 January 2019, <http://infed.org/mobi/peter-senge-and-the-learning-organization/>.

investment, and collaborative actions among key stakeholders; or at the national level is interagency..¹⁴⁸ The following discussion will observe the potential solution in addressing interoperability challenge utilizing leadership and organizational approach.

Leadership Approach: Recognize Risk and Adaptability Capability

BSSN and other agency leaders which rely on ICTs are to have robust intuition and thoughts to recognize risks. In achieving that level of thorough understanding, leaders must acknowledge what aspects can cause risks to obtain a clear situation of the environment to address those risks. A scholar asserts that risks are heightened during transferring resources and through the intensity of violent actions; in this thesis is being translated to cyber threats..¹⁴⁹ He mentions there were many times that transitions happened to cause actions being vulnerable and requiring more robust protection and concealment..¹⁵⁰ BSSN in this case also requires a robust protection system from the intensified cyber threats that attack depending on their interest.

Leaders must be able to mitigate risks. Porter asserts that situational understanding is essential to managing all risks, which can be achieved by enhancing organizations interoperability to identify risk, anticipate change, and adapt to the

¹⁴⁸ Schwab and Davis, *Shaping the Future of the Fourth Industrial Revolution*, 106.

¹⁴⁹ Scott A. Porter, M313 Reading A: Large-Scale Combat Operations: Risk and Adaptability at the Corps and Division Levels, Advanced Operations Course (AOC), Module III: Transition to the Offense the Art of Command (U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2018), 2.

¹⁵⁰ Ibid.

changing conditions. Interoperability provides leaders a comprehensive situational understanding to be able to identify assumptions and reorganize their thoughts. However, to achieve interoperability within or inter-organization, leaders are to perform effective interpersonal skills and power, understand organization climates and cultures, and leverage universal military solidarity with a common purpose to build strong coalitions. Without effective collaboration with other national agencies, BSSN would never gain situational awareness and rapidly adapt to changing environments.

Leaders are to be able to adapt to changing circumstances. The most adaptive organizations possess a healthy climate and culture which has an adaptive attitude and encourages open-mindset, innovative, and creative thoughts to adjust to the ever-changing environment. Porter describes this situation by stating no issue is too sensitive to discuss throughout the chain of command of agency creating emotional tranquility for everyone to think and speak. In a rapid changing environment, the effective actions are mostly achieved by allowing employees to contribute to developing both creative and sharp decisions. The role of expertise and functional staffs is essential to interpret their intent in facing uncertain, complicated, and complex situations.

All in all, risks are always associated with any actions. The agency or organization's adaptability, interoperability, and positive environment to achieve situational understanding are the primary requirements to address those risks.

Leadership Approach: Establishing a Sense of Urgency and Guiding Coalition

Kotter asserts that a sense of urgency and guiding coalition are the two fundamental aspects for shaping climate, culture and commitment of agencies. It is

portrayed by the eight-steps of Kotter's Model.¹⁵¹ Influences to enhance a sense of urgency and guiding coalition are crucial for both internal BSSN as a new-transformed agency and external cooperation in coordinating all agencies which have roles in the National Cyber Security Strategy.

Influences start by the thorough understanding of the sources influencing power inside BSSN. It is argued that the soft influencing techniques or rationale provide the most effective approach for obtaining commitment and shaping climate and culture of the current BSSN environment when associated with the decent inspiration methods. The emotional intelligence provides multiplayer effect in improving the influence techniques. BSSN must be adaptive and innovative in a cyberspace expected culture that thrives on stability and consistency. A culture of education and training involves leaders devoted to knowledge to enhance BSSN's capacity building, simultaneously to achieve the expected outcomes.

The leaders from the lowest to the top level of BSSN need to establish the sense of urgency for shaping climate and culture of this organization. Since BSSN is an integrated-institution from three distinct agencies, the sense of urgency is required from each previous umbrella of organizations. Leaders, staffs and employees are the components for shaping that climate and culture to achieve those objectives. Externally, establishing a sense of urgency and creating a guiding coalition are the primary aspects to achieve interoperability interagency. BSSN needs to develop an operational guidance to navigate the ways of implementing the National Cyber Security Strategy's strategic

¹⁵¹ John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 21.

vision for leading change. It is required to have an outline that provides a holistic and practical direction to achieve the National Cyber Security Strategy's objectives from all stakeholders associated.

Creating the guiding coalition encompasses all efforts to put groups to lead the transformation and create a coordination and cooperation system model.¹⁵² A group effort to lead the transformation is an inner power to achieve interagency interoperability. "That coalition—a powerful, enthusiastic team of volunteers from across an organization—is a crucial tool for leaders looking to put new strategies into effect and transform their organizations; and deciding who should take part in the guiding coalition is essential."¹⁵³ Groups, in achieving national cyber resilience, refer to ministries and agencies that enable the achievement of government's roles in the National Cyber Security Strategy created by BSSN in 2017. By observing government's roles and its cyber capability development concept, there are several ministries and agencies that potentially participate in leveraging national cybersecurity strategy. The ministries and national agencies included in Table 7 have been listed concerning its role in national administration including Ministry of State Secretariat/Cabinet Secretariat, Ministry of Defense/Armed Forces, Ministry of Finance/Bank of Indonesia, Ministry of Health, Ministry of Energy and Mineral Resources, Ministry of Transportation, Ministry of Agriculture, Coordinating Ministry for Political, Legal and Security Affairs, Ministry of

¹⁵² Kotter, *Leading Change*.

¹⁵³ Kotter Contributor, "Guiding Coalition: A Dream Team to Help You Implement Strategy Quickly," *Forbes*, 8 February 2012, accessed 25 February 2019, <https://www.forbes.com/sites/johnkotter/2012/02/08/guiding-coalition-a-dream-team-to-help-you-implement-strategy-quickly/#63c7f87db294>.

Religion, Ministry of Social. Conversely, it is arranged by its role in cyber or ICT system including BSSN and Ministry of Communication and Information Technology.

Table 7. Government's Roles		
Roles		Ministry/Agency
1	Protecting the national cyber environment,	BSSN
2	Protecting national e-Commerce,	Ministry of Communication and Information Technology
3	Protecting national critical information infrastructure,	(as below)
	a. Government	1) Secretariat of Cabinet 2) Ministry of Home Affairs
	b. Defense and Security	1) Ministry of Defense/Armed Forces 2) National Police 3) Indonesian Maritime Security Agency
	c. Banking	Ministry of Finance / Bank of Indonesia
	d. Health	Ministry of Health
	e. Energy and Mineral Resources	Ministry of Energy and Mineral Resources
	f. Transportation	Ministry of Transportation
	g. ICT	Ministry of Communication and Information Technology
	h. Food security	Ministry of Agriculture
4	Control penetration concerning ideology, politic, social, cultures, and national defense and security	a. BSSN b. Ministry of Defense c. Armed Forces d. National Police e. Ministry of Religion Affairs f. Ministry of Social Affairs g. Ministry of Education and Culture h. Ministry of Research, Technology, and Higher Education i. Ministry of Religious Affairs j. Ministry of Female Empowerment and Child Protection
5	Protecting Citizen / Privacy	Ministry of Communication and Information Technology

Source: Created by author using data from Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

Table 8. Government Development Program		
Capabilities Development		Ministry/Agency
1	Cyber intelligence	• Indonesian State Intelligence Agency • Armed Forces • National Police
2	Cyber defense	• Ministry of Defense • Armed Forces
3	Cybercrime	• Attorney General • National Police
4	Cyber diplomacy	Ministry of Foreign Affairs
5	Cyber economy	• Ministry of Communication and Information Technology • Ministry of Trade • Ministry of Industry • Ministry of Cooperatives and Small & Medium Enterprises • Ministry of State-Owned Enterprises

Source: Created by author using data from Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

These ministries and agencies listed should develop sense of urgency internally for enabling a guiding coalition achievement. The involvement and role of stakeholders are crucial since taking care of all cyberspace cannot be done discretely.¹⁵⁴ Indonesia needs to increase both the function and protection for the massive scheme in increasing national economic development. Cooperation and coordination are crucial because in achieving a national cyber resilience, Indonesia should have a measurement system that inhibits how diverse national elements function together and how its interoperability generates or fails to engender digital resilience based on national policies and strategy.

¹⁵⁴ The Ministry of Communication and Information Technology of Republic of Indonesia, *BSSN Jadi Lembaga Utama Keamanan Siber*.

Organizational Approach: A Networking Model

There are significant problems that change the world. If we are working together, that will make us understand each other, appreciate each other, help each other.

— Jack Ma, founder of Alibaba Group

The second step after developing sense of urgency would be defining the roles and responsibilities of agency in protecting national interest from cyber risks and threats. It is crucial to acknowledge their capability and limitation of capability to develop a comprehensive competence and capacity. Therefore, a networking model is essential for implementing National Cybersecurity Strategy.

BSSN needs a networking cooperation model with other agencies to conversely provide substantial support in cybersecurity matters throughout national, regional, and international scope. In tailoring Indonesia cyber resilience, an interagency partnership is one of the primary efforts. Interoperability is crucial to support the implementation of data and information exchanges between agencies so that it will facilitate the process of data sharing and the realization of more efficient and effective data utilization. It increases the capability of identification, detection, protection, mitigation, recovery, monitoring, evaluation, electronic-based trade protection control, coding, screening, cyber diplomacy, cyber crisis management center, cyber contact center, information center, mitigation support, recovery of vulnerability control, incidents, and cyber-attacks. The interoperability will improve effective and efficient efforts to support strategic decision-making in protecting national security. The interoperability requires less financial effort, but it demands strong commitment and integrity among agencies.

There are some considerations for establishing a networking model. First, it is a necessity to analyze what ministry, department, institution, and agency that can enable

the achievement of National Cybersecurity Strategy portrayed on Tables 7 and 8. To create a comprehensive understanding about overall government participation to increase cyber resilience capacity, decision makers should collaborate government's roles and its development in determining what ministry or agency that has responsibility toward respective tasks and purposes; what assets they have; and how to arrange these to achieve a unity of effort. That approach purposes to enhance the government's understanding of mapped network following conducting cooperation with the third party. Second, there are two key designs for conducting interagency partnerships. The interagency partnerships are formed by sharing assets or by sharing information between ministries, departments, and public institutions.¹⁵⁵ It needs a chain of command in accordance to specific matters to avoid overlapping job descriptions and protect the classified information or privacy credentials of each ministry or cyber sub-agencies capable of understanding virtual information. Having listed the government's roles in leveraging national cyber resilience, Indonesia's awareness of cyber threats is significant. The President of the Republic of Indonesia created the National Cyber and Crypto Agency as the principal organization to consolidate cyber component functions in ministries, departments, and institutions. The president' statement will facilitate the synchronized and capable system to achieve a unity of effort to conduct cyber resilience by integrating the existing component to achieve more significant effects on resilience capacity. Cooperation and coordination systems will formulate the unified action toward common objectives to support national critical functions and infrastructure as well as to protect those affairs.

¹⁵⁵ The Ministry of Communication and Information Technology of Republic of Indonesia, *BSSN Jadi Lembaga Utama Keamanan Siber*.

Based on that, the author analyzes a way for a comprehensive approach of Indonesia interagency cyber networking model. Figure 19 represents that coordinating ministries, ministries, other agencies, and BSSN as part of LPNK are under and responsible directly to the President of Republic of Indonesia. BSSN, as the center of government in cyberspace affairs, has a role to harmonize and synergize stakeholders which participate in national security and increasing national economic growth. BSSN must be capable of facilitating government's roles achievement and enable national cyber development to achieve the end states of the National Cyber Security Strategy. Importantly, the BSSN has a direct coordination with ministries and other agencies that support government's roles in protecting the national cyber environment, national E-commerce, and national critical information infrastructure. The illustration also explains BSSN coordination with ministries and agencies that has responsibility to control penetration concerning ideology, politics, social concerns, and cultures. Moreover, the blue-highlighted color identifies ministries and agencies that requires cyber development system for leveraging national cyber resilience capacity. Overall, that government network system is expected to create national defense and security in cyberspace, enhancing economic growth, and protecting Indonesian online privacy. Furthermore, it also depicts how the cyber government system linkage to other nomenclatures of cyber contemporary architecture is based on the National Cyber Security Strategy 2017.

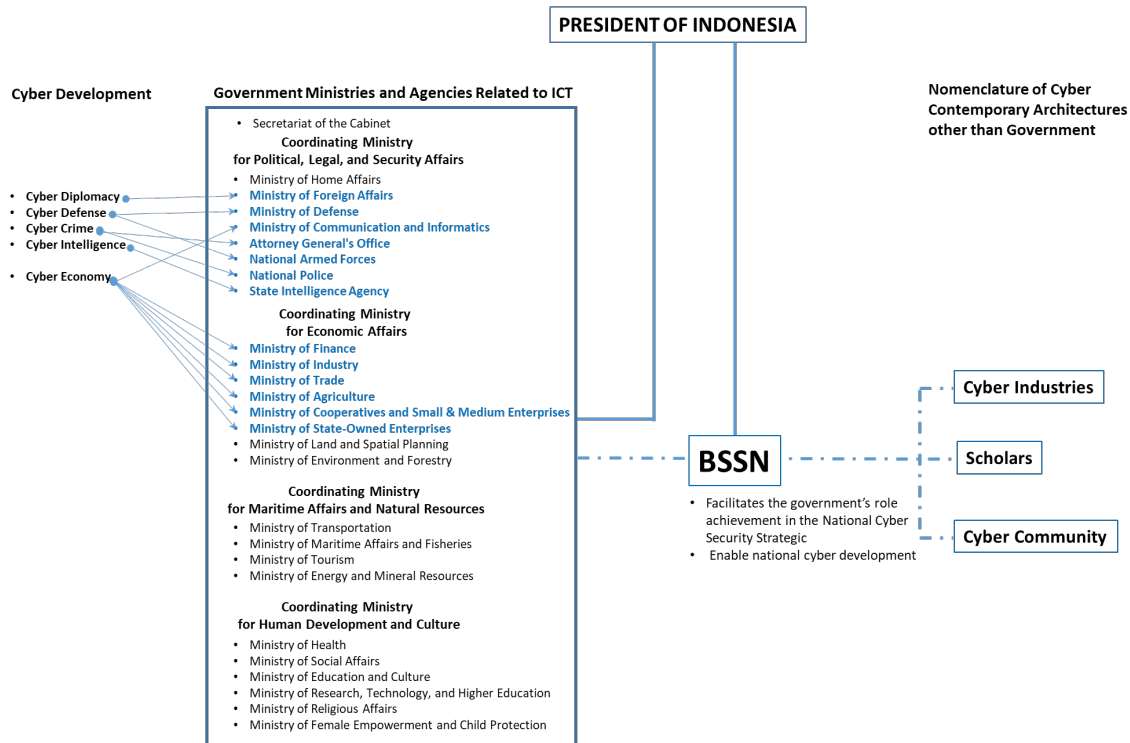


Figure 17. An Analysis of Comprehensive Approach of Cyber Networking Model Indonesia Interagency

Source: Create by author using data from Badan Siber dan Sandi Negara (BSSN), *Strategi Keamanan Siber Nasional* (Jakarta: Deputy III for Prevention and Recovery of BSSN, 2017).

Coordination and interagency cooperation are significant to reach national strategic objectives in the cyberspace because of its worldwide novelty. However, without a formal regulation to develop a hub coordinating system, coordination among each agency is more smoothly executed on paper than in real time. Even after establishing a rule to develop that system, it requires strong and robust commitment and effort to get it accomplished.

The vulnerability of security and confidentiality data from being breached, attacked, or spied increases because of data sharing and connectivity.¹⁵⁶ The necessity of new security frameworks of government agencies, corporations, and industrial internets becomes urgent to address this essential issue and create a resilience cyber capacity and capability including the response model. The lack of interoperability among existing stakeholders would potentially increase the complexity of problems and the cost of Industrial Internet deployments.¹⁵⁷

No country on earth is immune to cyber-attacks. There should always be a significant effort to tailor and leverage their cyber resilience capacity. The primary requirement is that the country has to know and understand its complex network mapped thoroughly.¹⁵⁸ That network model should be frequently revitalized to generate a dynamic chart for dynamic systems that intensely supports addition, change, or even removal of components within the system.¹⁵⁹ To execute that, governments and stakeholders or a third party have to impose directing policy concerning their linkages and procedures in respective national functions. They should be capable of determining any defects and chains of vulnerability that quickly knockout those threats.¹⁶⁰

¹⁵⁶ The World Economic Forum, “Industrial Internet of Things - Unleashing the Potential of Connected Products and Services,” 10.

¹⁵⁷ Ibid.

¹⁵⁸ Rothrock, *Digital Resilience*, 147.

¹⁵⁹ Ibid.

¹⁶⁰ Ibid., 148, 153.

The thorough understanding of its complex and complicated network map provides necessary consideration in developing a well-structured network. It analyzes the potential enemy course of action to identify and attack through a pathway of a country's system's chain of vulnerability. The next step the network systems are to evaluate is its infrastructures, strength, and weakness and ensure all assets are well-managed and arranged. The more understanding the source of attacks is, the easier and quicker to recover and re-operated. These are the fundamental concepts of cyber resilience.

All in all, situations above depict the urgency of interagency cooperation efforts to encounter numerous indecencies of those risks and threats. It is echoed to Indonesian proverb, "united we stand, divided we fall." Indonesia needs a framework of national cyber cooperation coordination model for implementing the operational guidance for operating efficiently and effectively.

Organizational Approach: Forming a National Operational Guidance or Regulation

Major transformations are often associated with one highly visible individual. Because major change is so difficult to accomplish, a power force is required to sustain the process.

— John P. Kotter, *Leading Change*

Indonesia needs operational guidance for implementing synchronization, coordination, and cooperation inter cyber-agency to achieve national unity and comprehensive effort. The higher level of urgency, the higher level of regulation to implement the National Cyber Security Strategy. Additionally, based on earlier analysis, cyberspace contributes significant advantages for achieving national objectives and interest; yet, it also suffers from its threats. The existing National Cybersecurity Strategy provides the strategic guidance; however, it might need a more robust regulation

concerning the comprehensive government's roles and its development scheme. A national model as a framework of coordination and harmonization in national cyberspace is one of the key requirements, but it needs regulation to make it happen.

The level of strategy and operational regulation is depending how Indonesia prioritizes its cyber affairs compared to other national functions or power. It is requiring a more profound and more thorough thought when it comes across to the national budget, national priority, and national comprehensive plan. The vigorous level of effectiveness cyber resilience can also be varied depending on the threats, commitment, and national capability. As mentioned earlier, the sources of threats can also be diverse depending on its actors, motives, and vulnerability. The description of how harmful the threats can also be described from the real-world attack or war: "limited war" vs. "total war." Those levels of war are distinguished based on strong intention or patriotism, larger armies, multi-echelon organization, budget committed on sustainment and enabler system, and the type of lethal weapons to attack. There are some instances from War World II history. First, allies that demanded unconditional surrender and completely defeated Axis powers committed all possible means and high cost on the primary reasoning of national survival. Second, the United States committed "limited war," but sought "total war" effects by committing large scale combat operations during the Desert Storm Operation to defeat Iraqi Forces. Third, in August 1945, the United States used a nuclear bomb on Hiroshima and Nagasaki that "wrestled the concept of limited war in the nuclear age. These types of war attacks conducted were based on purpose and considered the resilience capacity of the enemy to counterattack or at least remain to survive. The cyberspace is likewise, depending on the political situation and decision maker. However, as discussed earlier,

Indonesia needs to improve its cyber resilience capacity by tailoring its interagency operability.

In tailoring Indonesia cyber resilience, interagency partnership is one of the primary efforts. Interoperability is crucial to support the implementation of data and information exchanges between agencies so that it will facilitate the process of data sharing and the realization of more efficient and effective data utilization. It increases the capability of identification, detection, protection, mitigation, recovery, monitoring, evaluation, electronic-based trade protection control, coding, screening, cyber diplomacy, cyber crisis management center, cyber contact center, information center, mitigation support, recovery of vulnerability control, incidents, and cyber-attacks. The interoperability will improve the effective and efficient efforts to support strategic decision-making in protecting national security. Lesson learned from the GCI 2017 and World Economic Forum's research provides a distinct observation about challenges that might be encountered in leveraging Indonesia's cyber resilience capacity by tailoring its interagency partnership. Those challenges are the most concerning aspects in accordance to the existence of BSSN as the new-transformed organization assimilated by three different agencies.

To sum up, leadership and organizational approach are essential to leverage interagency interoperability system. A strong leadership will be able to visualize environment and gain situational understanding to analyze risks and create adaptability and make decisions to shape organization commitment and compliance to achieve objectives. To achieve a comprehensive approach, the government needs to officially

build a networking cooperation system and regulation to simultaneously shape a strong interoperable, reliable, and secure environment.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Interagency interoperability is one of the keys for achieving the Indonesia National Cyber Security Strategy's objectives. Interagency interoperability can provide a national comprehensive approach in benefiting cyberspace advantageous and simultaneously deter enormous cyber threats in national and international levels that can disrupt and destroy a country before it improves. BSSN, the Indonesia National Cyber Agency, is the government main effort to achieve a national cyber resilience capacity and capability to sustain economic growth and enable cyber innovation and creativity to protect national cyberspace. Expected as the new umbrella of national cyber center, as new agency, BSSN might encounter potential challenges in accordance to building climate, culture, and commitment.

Leadership and organizational approaches are the essential elements to mitigate the interoperability issues. Recognizing risks, adaptability, establishing a sense of urgency, building a guiding coalition and trusts are essential elements for enhancing a positive environment to achieve the desired climate, culture, and commitment. It is not only needed within BSSN, but also among ministries, departments, and agencies which performs in accomplishing the government's roles and development program in succeeding the National Cyber Security Strategy. Moreover, to achieve a comprehensive and simultaneous approach the government is required to officially build a networking model and regulation to shape a strong interoperable, reliable, and secure environment.

Recommendations

1. The Indonesian government should select one from two existing concepts of National Cyber Security Strategy that were established by the Ministry of Communication and Information Technology in 2016 and by BSSN in 2017. If possible, the National Cyber Security Strategy should be enacted by the president to create a more robust interoperability among ministries and national agencies which have roles to perform in successfully acquiring the cyber resilience capacity.

2. The Indonesian government should establish a model framework for the interagency cooperation as core element of the operational guideline, to enable interagency coordination and cooperation so that joint programs can run effectively and efficiently. Moreover, this coordination system model should be endorsed by a national regulation.

BIBLIOGRAPHY

Books

- Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.
- Farwell, James P., and Rafal Rohozinski. *Stuxnet and the Future of Cyber War*. London, UK: Routledge, 2011.
- Fels, Enrico. *Shifting Power in Asia-Pacific? –2017. The Rise of China, Sino-US Competition and Regional Middle Power Allegiance*. New York: Springer, 2017.
- Heinl, Caitríona H. *Regional Cybersecurity: Moving toward a Resilient ASEAN Cybersecurity Regime*. Washington: National Bureau of Asian Research, July 2014.
- Maier, Charles S. *Once Within Borders Territories of Power, Wealth, and Belonging since 1500*. Boston, MA: Harvard University Press, 2016.
- Romm, Joseph J. *Defining National Security*. New York: Council on Foreign Relations Press, 1993.
- Rothrock, Ray A. *Digital Resilience*. New York: American Management Association, 2018.
- Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber-Warfare*. New York: Cambridge University Press, 2013.
- Schwab, Klaus, and Nicolas Davis. *Shaping the Future of the Fourth Industrial Revolution*. Geneva, Switzerland: World Economic Forum, 2018.
- Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs To Know*. New York: Oxford University Press, 2014.
- Zweers, Louis. *Agressi II: Operatie Kraai. De Vergeten Beelden van De Tweede Politionele Actie*. Netherland: SDU Uitgevers, 1995.

Government Documents

- Badan Siber dan Sandi Negara (BSSN). *The National Cyber and Crypto Agency Regulation Number 2 of 2018 Concerning Organizations and Work Procedures for National Cyber and Crypto*. Jakarta: BSSN, 2018.
- . *Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara*. Jakarta: BSSN, 2018.

———. *Strategi Keamanan Siber Nasional (National Cyber Security Strategy.)* Jakarta: BSSN, 2017.

The Coordinating Ministry for Political Legal and Security Affairs of Republic of Indonesia. *Menko Polhukam dan BSSN Bahas Sinergitas Siber*. Jakarta: The Coordinating Ministry Polhukam Public Relations Bureau, 21 January 2018.

The Directorate General for Postal and Information Technology Affairs. *Annual Report*. Jakarta: The Directorate General for Postal and Information Technology Affairs, 2014.

The Indonesia National Police. *The Indonesia National Chief of Police' Decree of number 54 / X / 2002*. Jakarta: The Indonesia National Police, 17 October 2002.

Komite Nasional Indonesia Pusat (KNIP). *The Preamble of the Constitution of the Republic of Indonesia 1945*. Jakarta: KNIP, 29 August 1945.

The Ministry of Communication and Information Technology of the Republic of Indonesia. *Jumlah Pengguna Internet 2017 Meningkat, Kominfo Terus Lakukan Percepatan Pembangunan Broadband*. Jakarta: The Ministry of Communication and Information Technology, 19 February 2018.

The Ministry of Defense of the Republic of Indonesia. *Defense White Paper*. Jakarta: The Ministry of Defense of the Republic of Indonesia, 2015.

———. *State Gazette of the Republic of Indonesia, No.1712- Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014*. Jakarta: The Indonesia Ministry of Law, 17 October 2014.

The National Policing Improvement Agency. *Guidance on Multi-Agency Interoperability*. Bedfordshire, UK: Association of Chief Police of Officer, 2009.

The President of the Republic of Indonesia. *The Law of the Republic of Indonesia Number 39 of 2008*. Jakarta: The Ministry of State Secretariat, 2008.

U.S. Joint Chiefs of Staff. Joint Publication 3-12, *Cyberspace Operations*. Washington DC: US Government Printing Office, 5 February 2013.

Online Government Resources

Badan Siber dan Sandi Negara (BSSN). "Remarks the Chief of BSSN about Indonesian National Cyber Security Strategy." 2018. Accessed 31 December 2018.
<https://bssn.go.id/strategi-keamanan-siber-nasional/>.

Brangwin, Nicola. *National Security—Cybersecurity*. Canberra: Commonwealth of Australia, 2016. Accessed 15 November 2018.
https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/Cybersecurity.

- Chendramata, Aidil. *Indonesia Cyber Security Strategy*. Jakarta: Directorate of Information Security. The Ministry of Communication and Information Technology of Republic of Indonesia, 2016. Accessed 17 January 2019. http://dephub.go.id/public/files/uploads/posts/posts/postbody/strategi_cs_nasional_desember2016.pdf.
- Coats, Daniel R. *World Wide Threat Assessment of the US Intelligence Community* Statement for the Record. Washington, DC: Director of National Intelligence, 13 February 2018. Accessed 25 January 2018. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.
- Id/SIRTI-CC. *Pasukan Cyber Indonesia Harus Dipimpin Presiden!* Jakarta: Id/SIRTI, 2014. Accessed 17 December 2018. <https://idsirtii.or.id/berita/baca/48/pasukan-cyber-indonesia-harus-dipimpin-presiden-.html>.
- The Ministry of Communication and Information of Singapore. *Singapore's Cybersecurity Strategy*. Singapore: CSA Singapore, 2016. Accessed 15 November 2018. <https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy>.
- The Ministry of Communication and Information Technology of Republic of Indonesia. *BSSN Jadi Lembaga Utama Keamanan Siber*. Jakarta: Kominfo, 5 June 2017. Accessed 8 November 2018. https://www.kominfo.go.id/content/detail/9800/bssn-jadi-lembaga-utama-keamanan-siber/0/sorotan_media.
- Office of the Director of National Intelligence. "About the ISE." 2018. Accessed 24 January 2019. <https://www.ise.gov/blog/kshemendra-paul/coordinating-cybersecurity-programs>.
- Schneider, Grant. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years." The White House. 20 September 2018. Accessed 13 December 2018. <https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years>.
- U.S. Census Bureau. "U.S. and World Population Clock." 14 December 2018. Accessed 13 December 2018. <https://www.census.gov/popclock/>.
- U.S. Department of State, Bureau of East Asian and Pacific Affairs. "U.S. Relations with Indonesia." Fact Sheet. 14 August 2018. Accessed 30 January 2019. <https://www.state.gov/r/pa/ei/bgn/2748.htm>.

Organizations

- The Australia Strategic Policy Institute. *Cyber Maturity in the Asia-Pacific Region 2017*. Barton ACT, Australia: International Cyber Policy Centre, December 2017.

- California Environmental Associates. *Trends in Marine Resources and Fisheries Management in Indonesia: A 2018 Review*. August 2018. Accessed 9 February 2019. <https://www.packard.org/wp-content/uploads/2018/08/Indonesia-Marine-Full-Report-08.07.2018.pdf>.
- Ernst and Young. *The Role of Green ICT In Enabling Smart Growth in Estonia*. Tallinn: The Ministry of Economic Affairs and Communications of Estonia, 2012. Accessed 25 October 2018. http://www.mkm.ee/public/Inno_18_GreenICT.pdf.
- European Commission. *Accompanying the Document Proposal for a Directive of the European Parliament and the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union*. Impact Assessment. Strasbourg: European Commission, 7 February 2013.
- G20 Germany 2017. *2017 Growth Strategy –Indonesia*. Accessed 15 January 2019. https://www.bundesfinanzministerium.de/Content/DE/Downloads/G20-Dokumente/Hamburg_Wachstumsstrategien/IDN-Growth-Strategy.pdf_blob=publicationFile&v=4.
- Huawei Technologies Co. “Global Connectivity Index 2018: Tap into New Growth with Intelligent Connectivity.” 2018. Accessed 25 December 2018. https://www.huawei.com/minisite/gci/assets/files/gci_2018_whitepaper_en.pdf?v=20180914.
- The International Monetary Fund. “Measuring the Digital Economy.” 28 February 2018. Accessed 11 February 2019. <https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy>.
- The International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2017*. Geneva, Switzerland: ITU, 2017.
- The International Telecommunication Union. *Series X: Data Networks, Open System Communications, and Security Telecommunication Security - Overview of Cybersecurity*. Recommendation ITU-T X.1205. 2 April 2008. Accessed 9 February 2019. <https://www.itu.int/rec/T-REC-X.1205-200804-I>.
- Keidanren (Japan Business Federation). *Toward the Realization of The New Economy and Society - Reform of the Economy and Society by the Deepening of “Society 5.0.”* 28 April 2016. Accessed 9 January 2019. http://www.keidanren.or.jp/en/policy/2016/029_outline.pdf.
- Kotter Contributor. “Guiding Coalition: A Dream Team to Help You Implement Strategy Quickly.” *Forbe.*, 8 February 2012. Accessed 25 February 2019. <https://www.forbes.com/sites/johnkotter/2012/02/08/guiding-coalition-a-dream-team-to-help-you-implement-strategy-quickly/#63c7f87db294>.

Microsoft Asia News Center. “Malware Infection Index 2016 Highlights Key Threats Undermining Cybersecurity in Asia Pacific: Microsoft Report.” Microsoft. 7 June 2016. Accessed 21 April 2019.

<https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/>.

Symantec Corporation. *The 2017 Norton Cyber Security Insights Report*. Tempe, AZ: Symantec, 2017.

———. *Internet Security Threat Report (ISTR) Government*. November 2017. Accessed 27 April 2019.

<https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf>.

The United Nations Development Programme (UNDP) Indonesia Country Office. *Converging Development Agendas: ‘Nawacita,’ ‘RPJMN,’ and SGDs*. UNDP, November 2015. Accessed 30 January 2019.
<http://www.id.undp.org/content/dam/indonesia/2015/doc/publication/ConvFinal-En.pdf>.

The World Bank. “Remarks by World Bank Group President Jim Yong Kim at the 2018 Annual Meetings Plenary.” Jakarta, 12 October 2018.

The World Economic Forum. “Industrial Internet of Things - Unleashing the Potential of Connected Products and Services.” Industry Agenda. Geneva, January 2015. Accessed 6 February 2019.
http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

Reports

Das, Kaushik, Michael Gryseels, Priyanka Sudhir, and Khoon Tee Tan. “Unlocking Indonesia’s Digital Opportunity.” McKinsey & Company, October 2016. Accessed 25 April 2019. https://www.mckinsey.com/~media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. *Cyber Readiness Index 2.0 A Plan for Cyber Readiness: A Baseline and an Index*. Arlington, VA: Potomac Institute for Policy Studies, November 2015. Accessed 14 October 2018. <http://www.potomac institute.org/images/CRIndex2.0.pdf>.

Keys, Brianna, Aashish Chhajaj, Zilong Liu, and Daniel Horner. *A Framework for Assessing Cyber Resilience*. Geneva: World Economic Forum, 2016. Accessed 13 February 2019. http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf.

Nichol, Jim. *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interest*. CSR Report to Congress. Washington, DC: Congressional Research Service, 3 March 2009. Accessed 2 December 2018.
<https://fas.org/sgp/crs/row/RL34618.pdf>.

Papers

Hathaway, Oona A., and Rebecca Crootof. "The Law of Cyber-Attack." Yale Law School Faculty Scholarship, 2012. Accessed 21 April 2019.
https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4844&context=fss_papers.

Ricketts, Tim. "Sheep Dip Your Removable Storage Devices to Reduce The Threat of Cyber Attacks." M.A.C Solution, 2019. Accessed 12 April 2019.
<https://www.mac-solutions.net/en/news/129-sheep-dip-your-removable-storage-devices-to-reduce-the-threat-of-cyber-attacks>.

Ridho, Faizin, Anton Yudhana, and Imam Riadi. "Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Denial of Service (DDoS) Secara Real Time." Annual Research Seminar 2016, Ahmad Dahlan University, Yogyakarta, Indonesia, 6 December 2016.

Online Sources

Alimova, Alina and Nicholas Goggin. "The G20 Summit Explained." *Atlantic* (blog) *Atlantic Council*. 29 November 2018. Accessed 2 February 2019.
<https://www.atlanticcouncil.org/blogs/new-atlanticist/the-g20-summit-explained>.

Anggraini, Ervina. "Indonesia's Vision: 1,000 Startups By 2020." *Digital News Asia*, 27 November 2015. Accessed 6 November 2018. <https://www.digitalnewsasia.com/indonesias-vision-1000-startups-2020>.

Barrett, Devlin, Danny Yadron, and Damian Paletta. "U.S. Suspects Hackers in China Breached about 4 Million People's Records, Officials Say." *Wall Street Journal*. 5 June 2015. Accessed 19 April 2019. <https://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888>.

Bhunja, Priyankar, "Exclusive" Safeguarding Malaysian Cyberspace (Part II) – International Cooperation, Changing Mindsets." Open Gov. Accessed 6 February 2019. <https://www.opengovasia.com/exclusive-safeguarding-malaysian-cyber-space-part-ii-international-cooperation-changing-mindsets/>.

Björck, Fredrik, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. "Cyber Resilience – Fundamentals for a Definition." *Advances in Intelligent Systems and Computing* 353 (1 January 2015): 311-316. Accessed 25 December 2018.
https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition.

- Bohang, Fatimah Kartini, "Berapa Jumlah Pengguna Internet Indonesia?" *Kompas*. 22 February 2018. Accessed 6 November 2018.
<https://tekno.kompas.com/read/2018/02/22/16453177/berapa-jumlah-pengguna-internet-indonesia>.
- Chopra, Ambika. "Sustainable Tourism, Startups, and Innovation: A Glimpse into Indonesia Startup Weekend." *Inc42*. 8 June 2017. Accessed 1 February 2019,
<https://inc42.com/indonesia/startup-weekend-indonesia/>.
- Cîrnu, Carmen Elena. "Cyber Diplomacy – Addressing the Gap in Strategic Cyber Policy." *The Market for Ideas*. September-December 2017. Accessed 10 February 2019. <http://www.themarketforideas.com/cyber-diplomacy-addressing-the-gap-in-strategic-cyber-policy-a388/>.
- Coalson, Robert. "Behind the Estonia Cyberattacks." *RadioFreeEurope RadioLiberty*. 6 March 2009. Accessed 1 August 2018. https://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html.
- Craigen, Dan, Nadia Djakun Thibault, and Randy Purse. "Defining Cybersecurity." *The Technology Innovation Management Review* (17 October 2014): 13-21. Accessed 2 January 2019. https://www.academia.edu/9061472/Defining_Cybersecurity.
- Damar, Agustinus Mario. "Indonesia Alami 205 Juta Serangan Siber Sepanjang 2017." *Liputan6*. 22 December 2017. Accessed 6 November 2018.
<https://www.liputan6.com/tekno/read/3203987/indonesia-alami-205-juta-serangan-siber-sepanjang-2017>.
- Davis, Jessica, "Hackers Breach 1.5 Million Singapore Patient Records, Including the Prime Minister's." *HealthcareITNews*. 20 July 2018. Accessed 24 January 2019.
<https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers>.
- Denning, Steve. "How Do You Change an Organizational Culture?" *Forbes*. 23 July 2011. Accessed 12 January 2019. <https://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/#6c60781839dc>.
- Gewirtz, David. "Why The Next World War Will Be A Cyberwar First, And A Shooting War Second." *ZD Net Government*. 22 June 2015. Accessed 7 November 2018.
<https://www.zdnet.com/article/the-next-world-war-will-be-a-cyberwar-first-and-a-shooting-war-a-distant-second/>.
- Hern, Alex. "North Korea is A Bigger Cyber-Attack Threat Than Russia, Says Expert." *The Guardian*. 26 February 2018. Accessed 10 January 2019.
<https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia>.
- Hufnagel, Stephen. "Interoperability." *Military Medicine* 174, no. 43 (May 2009). Accessed 23 February 2019. https://academic.oup.com/milmed/issue/174/suppl_5.

- Indonesia Travel. "18th Asian Games A Resounding Success: Indonesia Praised Worldwide." 6 September 2018. Accessed 23 December 2018. <https://www.indonesia.travel/us/en/news/18-th-asian-games-a-resounding-success-indonesia-praised-worldwide>.
- Iswara, Raditya N. "Agresi Militer I: Saat Belanda Mengingkari Perjanjian Linggarjati," *Tirto.id*. 21 Juli 2018. Accessed 15 January 2019. <https://tirto.id/agresi-militer-i-saat-belanda-mengingkari-perjanjian-linggarjati-cs8T> 21 Juli 1947.
- Kelley, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*. 20 November 2013. Accessed 1 August 2018. <https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>.
- Mantra, IGN. "Tumpang Tindih Tugas Badan Siber Dengan Lembaga Lain." *Detikinet*. 8 January 2018. Accessed 16 October 2018. <https://inet.detik.com/security/d-3805210/tumpang-tindih-tugas-badan-siber-dengan-lembaga-lain>.
- Mite, Valentinas, "Estonia: Attacks Seen as First Case of Cyberwar." *RadioFreeEuropeRadioLiberty*. 30 May 2007. Accessed 13 December 2018. <https://www.rferl.org/a/1076805.html>.
- Perlroth, Nicole. "Who Is Selling Target's Data?" *The New York Times*. 24 December 2013. Accessed 19 April 2019. https://bits.blogs.nytimes.com/2013/12/24/who-is-selling-targets-data/?_r=0.
- Prasetya, Eko. "Dari 17.504 Pulau di Indonesia, 16.056 Telah Diverifikasi PBB." *Merdeka*. 19 August 2017. Accessed 6 November 2018. <https://www.merdeka.com/peristiwa/dari-17504-pulau-di-indonesia-16056-telah-diverifikasi-pbb.html>.
- Rachmatunnisa, "3 Tahun Jokowi-JK, Geber Ekonomi Digital Terinspirasi Silicon Valley." *Inet.Detik*. 20 October 2017. Accessed 6 November 2018. <https://inet.detik.com/cyberlife/d-3692537/3-tahun-jokowi-jk-geber-ekonomi-digital-terinspirasi-silicon-valley>.
- Santos, Jet Damazo. "The Big Picture: Indonesia's Partnership with U.S. Investors." *US Chamber*, November 2017. Accessed 6 November 2018. https://www.uschamber.com/sites/default/files/11.2017_investment_report_the_big_picture.pdf.
- Seals, Tara. "One Year After WannaCry: A Fundamentally Changed Threat Landscape." *Threat Post*. 17 May 2018. Accessed 26 January 2019. <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/>.

- Setiawan, Sakina Rakhma Diah. "Tahun 2017, Pengguna Internet di Indonesia Mencapai 143,26 Juta Orang." *Kompas*. 19 February 2018. Accessed 11 August 2018. <https://ekonomi.kompas.com/read/2018/02/19/161115126/tahun-2017-pengguna-internet-di-indonesia-mencapai-14326-juta-orang>.
- Smith, Mark K. "Peter Senge and the Learning Organization." Infed. Accessed 25 January 2019. <http://infed.org/mobi/peter-senge-and-the-learning-organization/>.
- Tisdall, Simon. "Joko Widodo Takes Office With Plans For Economic Growth and Political Clout." *The Guardian*. 20 October 2014. Accessed 6 November 2018. <https://www.theguardian.com/australia-news/2014/oct/20/joko-widodo-takes-office-in-indonesia>.
- Tumouto. "Jumlah Penduduk Indonesia Tahun 2018 (BPS Prediction)." *Tumoto News*. 5 October 2018. Accessed 6 November 2018. <https://tumoutounews.com/2018/05/10/jumlah-penduduk-indonesia-tahun-2018>.
- Yu, Eileen. "Singapore Suffers 'Most Serious' Data Breach, Affecting 1.5M Healthcare Patients Including Prime Minister." Zdnet. 20 July 2018. Accessed 26 January 2019. <https://www.zdnet.com/article/singapore-suffers-most-serious-data-breach-affecting-1-5m-healthcare-patients-including-prime/>.
- Yuniarni, Sarah. "Indonesia Had 143M Internet Users in 2017: APJII." *Jakarta Globe*. 19 February 2018. Accessed 6 November 2018. <https://jakartaglobe.id/business/indonesia-143m-internet-users-2017-apjii>.

Other Sources

- Crevelde, Martin Van. "Transformation of War Strategy in the 21st Century." Interview by Christina Schori Liang, Geneva Centre for Security Policy, 12 March 2018. Accessed 12 September 2018. <https://www.gcsp.ch/global-insight/transformation-war-strategy-21st-century>.
- Porter, Scott A. M313 Reading A, Large-Scale Combat Operations: Risk and Adaptability at the Corps and Division Levels, Advanced Operations Course (AOC). Module III: Transition to the Offense the Art of Command. US Army Command and General Staff College, Fort Leavenworth, KS, 2018.