THE FUTURE OF CYBER SECURITY Capacity in Indonesia

Top 20 Recommendations for Strengthening National Cybersecurity Capacity

1	Develop a National Cyber Security Strategy (NCSS).	6	Establish emergency response asset priorities, in the event of a service failure occurs, that aim at reducing impact.	11	Identify a centre of excellence in cybersecurity research and education to locate strengths and provide focused investment to address gaps.	16	Strengthen law enforcement and prosecutors' capabilities to investigate cybercrime and bring those responsible to justice.
2	Strengthen the Role and Coordination Function of ID-SIRTII/CC as a National CERT.	7	Develop a cybersecurity communication strategy o strengthen and expand the national cybersecurity campaign.	12	Promote cybersecurity training and education programmes designed for all employees at all levels of government organisations, state-owned enterprises, private critical infrastructure providers, and small-medium enterprises.	17	Create a single reporting system for electronic system operators for public services to report and disclose cybercrime incidents and data breaches so that action can be taken.
3	Create a Formal List of Critical National Infrastructure (CNI) on Multi-Stakeholder Consultation and work with the companies that own and manage CNI.	8	Develop a single authoritative online portal for cyber awareness-raising amongst governments agencies, businesses and civil society across the country.	13	Create a national level register for information assurance and cyber security experts across the public and private sector as a way of bringing new talent into the profession.	18	Promote cybersecurity requirements in government procurement processes for managing the national cyber defence.
4	Conduct crisis management exercises at a national level by inviting the relevant key national stakeholders, in order to ensure preparations for cyber incident responses are well managed and robust.	9	Promote greater levels of trust in online services, such as e-government and e-commerce services	14	Raise awareness amongst senior government officials and board members of the critical national infrastructure operators concerning the cyber risks	19	Establish a government unit under the related ministry to formally monitor and control national infrastructure to help ensure Indonesia's security and resilience.
5	Create and build a dedicated civilian and military capability to help ensure that Indonesia has the capability to protect national interests in cyberspace.	10	Develop a standard marketing strategy to promote privacy online for protecting personal data	15	Review existing legislation, for example amending the ITE law No.11/2008, to ensure that it remains relevant and effective in fighting cybercrime.	20	Provide incentive-based cybersecurity solutions for local cybersecurity products or cyber insurance marketplace.

Yudhistira Nugraha,
(Oxford Internet Institute/Centre for Doctoral Training in Cyber Security,University of Oxford)

Taylor Roberts,
(Global Cyber Security Capacity Centre, University of Oxford)

Professor Ian Brown,
(Oxford Internet Institute, University of Oxford)

Dr Ashwin Sasongko Sastrosubroto,
(Informatic Research Centre Indonesian Institute of Science and Centre for ICT Public Policy, Telkom University)

2016

Acknowledgements

This report was produced by the Oxford Internet Institute, the University of Oxford, under the supervision of Professor Ian Brown (Principal Investigator), using responses from a group selected for their expertise in the areas of CMM review, including policy makers, law enforcement, critical infrastructure owner, private sectors, incident response teams, national security and resilience organisations, academia, public administration organisations, and international organisations. It should be noted that group stakeholders participated as individuals. This paper should therefore not be taken as representing the official policy or position of the Government of Indonesia or as the views of other organisations, and individual group members may not agree with all of the observations and recommendations made in the report. The authors would like to thank Mr. Bambang Heru Tjahjono, Professor Muhammad Ashari, and Ms. Kautsarina, as well as the anonymous participants for their helpful support for, and participation in, this study. The cover was designed by Maydina Zakiah Siagian. This work was supported in part by the UK FCO under the Cyber Security Capacity Building Fund Programme – FY 2015/2016.

Written by Yudhistira Nugraha, Oxford Internet Institute, University of Oxford

Contributors:

Taylor Roberts, Global Cyber Security Capacity Centre, University of Oxford

Professor Ian Brown, Oxford Internet Institute, University of Oxford

Dr. Ashwin Sasongko Sastrosubroto, Informatic Research Centre, Indonesian Institute of Sciences and Centre for ICT Public Policy, Telkom University

March 2016

Contact: Oxford Internet Institute University of Oxford 1 St Giles Oxford OX1 3JS United Kingdom. Telephone: +44 (0) 1865 287210 Fax: +44 (0) 1865 287211

Please cite the source of text and data excerpts as: Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford Internet Instutite, University of Oxford.

Table of Contents

Revision History

Date	Version	Revised By	Comments
September 2016	1	YN	Update document for a full report.
March 2016			Initial Release

Foreword

I have been fortunate to have had almost six years of duty in the field of cybersecurity in Indonesia since I joined the Ministry of Communications and Information Technology in 2011 as the first Director of Information Security, to lead the new government unit for cybersecurity. Of course, it is such a new area that ‘’we do not know what we do not know’’. I often reflect on how different cybersecurity is compared with physical security in terms of regulation and raising awareness.

When the Indonesian delegation and I attended the first global conference on cyberspace in London in late 2011, which was attended by over 700 participants from 60 countries, including ministers, senior government officials, industry leaders, and representatives of the Internet technical community and civil society, all delegates agreed that the Internet must be secure and reliable so that government, industry, and civil society can conduct business with confidence. It is worth noting that the Internet has an important economic role to play as an engine and facilitator of economic growth and prosperity, especially in Indonesia. Internet technologies have proven to be a critical factor in productivity growth and innovation. We want to have the best-developed e-commerce in the ASEAN Economic Community, as the developments in the cyber domain are taking place at a rapid rate. Also, the potential and actual impact of cyber threats have become clearer, due to a number of highly publicised incidents. These threats may not only compromise our critical information infrastructure, but also the confidentiality, integrity, and availability of the security-sensitive information we process, transmit, and store online.

In order to be able to continue to respond to these threats, the Government of Indonesia plans to further strengthen and extend their cybersecurity capacity in terms of organisational structure and coordination. Also, the government has passed several national laws considered as the Indonesian cybersecurity legal framework, such as Law number 11/2008, Law number 36/1999, Law number 14/2008, Law number 25/2009, and the Government Regulation number 82/2012. However, the government requires a further development of effective laws and regulations to encourage the development and use of a secure Internet. In addition, it will be essential to raise the security awareness of Indonesian society, from school pupils, young adults, and employees, to IT specialists, board members, and government officials.

I am delighted that the Directorate General of ICT Applications, the Ministry of Communications and Information Technologies, has been able to support this white paper on the future of cybersecurity capacity in Indonesia. Its review and recommendations will fill gaps and highlight proposed actions to include for strengthening national cybersecurity capacity in the country. I am sure that this white paper will provide clear guidance to the Government of Indonesia in the development of a comprehensive policy and strategy on cybersecurity, for the security and prosperity of the country.

Jakarta, March 2016

Director General of ICT Applications
Bambang Heru Tjahjono

About the project

Through collaboration with the Indonesian Ministry of Communication and Information Technologies (MCIT) and Telkom University, the University of Oxford's Global Cyber Security Capacity Centre (GCSCC) has facilitated a review of the cybersecurity capacity of the Republic of Indonesia. The objective of this exercise is to enable the Indonesian Government to prioritise areas of capacity, which the country might strategically invest in to become more cyber secure and resilience.

The Cybersecurity Capacity Review of Indonesia was conducted in the form of focus group discussions (FGDs) with nine Indonesian stakeholder groups. The cybersecurity review provides a platform for the government, industry, and academic stakeholders to improve coordination, communication, and collaboration in Indonesia's cybersecurity policymaking activities. During the FGDs, the stakeholders were assigned to conduct the evaluation depending on their stakeholder grouping. These groupings assessed one or two dimensions of the GCSCC Capability Maturity Model (CMM). This white paper provides a basis for the Government of Indonesia to develop the country's national cybersecurity capacity. The project also contributes to the GCSCC's mission of assessing cybersecurity capacity globally, with the ultimate aim of enhancing strategic investment in cybersecurity capacity across nations.

The following 38 stakeholders participated in a three-day consultation for the review of cybersecurity capacity in Indonesia, while five individuals from UI, BI, OJK, RISTEKDIKTI, and JICA participated online through a survey:

1. National Crypto Agency (LEMSANEG)
2. Directorate of Information Security – KOMINFO
3. Ministry of Research, Technology and Higher Education (RISTEKDIKTI)
4. National ICT Council (DETIKNAS)
5. Ministry of Finance
6. Ministry of State Owned Enterprises (BUMN)
7. Ministry of Transportation

8. Ministry of State Secretariat
9. National Resilience Council
10. Indonesian National Armed Forces
11. National Narcotics Bureau (Badan Narkotika Nasional)
12. Agency For The Assessment And Application Of Technology (BPPT)
13. ITB-KOREA Cyber Security Research and Development Centre
14. Corruption Eradication Commission (KPK)
15. Cyber Crime Unit - The Indonesian National Police (POLRI)
16. ICT Research and Development Agency – KOMINFO
17. Secretariat of Directorate of ICT Applications – KOMINFO
18. Telkom University
19. University of Indonesia (UI)
20. PT Telkom Tbk
21. PT Indosat Oredo
22. PT XL Axiata
23. Central Bank of Indonesia (BI)
24. Indonesian Financial Services Authority (OJK)
25. PT PLN (National Grid)
26. PT Angkasa Pura II (Indonesia's Airport Company)
27. PT INTI (Indonesian Telecommunication Industry)
28. Indonesian Internet Service Providers Association (APJII)
29. Indonesian Chamber of Commerce and Industry (KADIN)
30. Klik Indonesia
31. Swiss German University
32. PT IBM Indonesia
33. PT OLX Indonesia
34. Indonesia-Security Incident Response Team on Internet Infrastructure
35. Government Computer Security Incident Response Team (Gov-CSIRT)
36. Academic CERT
37. PT Xynexis
38. Japan International Cooperation Agency (JICA)

Executive Summary

Cyberspace is a new domain and nervous system that requires a shared responsibility between stakeholders at the national and global levels. It consists of hundreds of thousands of interconnected computers, servers, routers, switches, and fibre optic cables that allow critical national infrastructures to work. It has supported the development of a borderless society, providing unprecedented opportunities to increase the wealth of the nation and stimulate economic growth.

Securing cyberspace is a challenge, which requires coordinated and focused effort from all key national stakeholders, as well as international stakeholders, ranging from policy makers, law enforcement, critical infrastructure owners, private sectors, incident response teams, national security and resilience organisations, academia, public administration organisations, and international organisations. It is clear that, for cybersecurity capacity-building to be successful, there must be a concerted global effort, as the Internet and cyberspace are global networks. Hence, it is in the interest of every country, including the UK, to enhance cybersecurity capacity around the world.

This study is a part of Oxford University's Global Cyber Security Capacity Centre's mission of using its cybersecurity CMM to help understand and improve cybersecurity capacity across countries in the world, including Indonesia. The study aims to identify and potentially fill gaps in cybersecurity capacity in Indonesia and globally by providing a comprehensive overview to be referred to by the key national stakeholders. It is in the interest of the UK that all countries, including Indonesia, have a national policy and strategy on cybersecurity, which will hopefully lead to the formulation of strategies and programmes. Also, this study is expected to create a better engagement of the UK and Indonesia on cyberspace issues. In the future, this study will help create a secure cyber ecosystem in the country, strengthen cybersecurity measures and the regulatory environment, enhance national computer

incident response, enhance awareness and improve skills of the stakeholders and society at large, develop a multi-stakeholder approach to cyber policy and strategy to combat cyber threats, and enhance regional, as well as international, cooperation in this field.

Based on our review of cybersecurity capacity in Indonesia, the 20 capacity factors range in maturity between the *start-up* and *formative* stages, with some factors on their way to the *established* stage, do not yet fully achieve all of the requirements of the stage.

- **D1-1. National Cybersecurity Strategy**: There is no evidence of a cybersecurity strategy existing in Indonesia. However, discussion processes through the Desk on Cyber Security have been established for key stakeholder groups. Some government organisations, such as POLHUKAM, KOMINFO, KEMHAN, LEMSANEG, and POLRI deal with cybersecurity components. However, a variety of cyber programmes have been designated within each of the government entities. Also, no formal focal point exists for cybersecurity coordination and development in Indonesia.
- **D1-2. Incident Response**: Though certain cyber threats have been categorised, they are not formally identified and recorded as national level incidents. A formal coordination or information sharing mechanism established with government entities is limited through Gov-CSIRT. Even though Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) is considered as CC (Coordinating Centre), the national incident response is limited and the response is still reactive. A coordinated national incident response is established through ID-SIRTII, but lines of communication remain ad hoc for crisis situations.
- **D1-3. Critical National Infrastructure (CNI)**: The Indonesian Ministry of Defence created a general list of CNI assets through a Roadmap for National Cyber Defence Strategy in 2013, but it was done without identified risk-based priorities and government consultation with key stakeholders. Moreover, there

is little evidence of interaction between government ministries and owners of CNI assets. Such discussions in the Indonesian National ICT Council and the Ministry of Defence have taken place to determine which industries and bodies are critical to the national cyber ecosystem. However, a lack of regular dialogue exists between tactical and executive strategic levels regarding cyber risks against CNI assets.

- **D1-4. Crisis Management**: There is a minimal crisis management at a national level, although ID-SIRTII regularly conducts the Drill test, in which some key stakeholders are involved. In this case, the test has been undertaken within a simple exercise scenario of attack, based on competition. Participants evaluate the exercise on an ad-hoc basis, but it does not feed into the decision-making process. Results of exercises also do not inform overall crisis management at the national level.
- **D1-5. Cyber Defence Consideration**: There is evidence that a national cyber defence strategy exists, outlining specific threats to national security in cyberspace, such as state-sponsored attacks and threats to defence and military operational capacity. However, a coordinated response strategy does not yet exist in practice. Thus, there is no clear command structure for cybersecurity in the Indonesian armed forces. In the case of a cyber-defence operation, the Ministry of Defence (KEMHAN) is responsible for defence during conflict using cyber means in cooperation with KOMINFO and ID-SIRTII.
- **D1-6. Digital Redundancy**: Digital redundancy measures are considered as security requirements, especially for public services. In most cases, standard operating procedures are established in the event of a communication disruption. However, a national cyber emergency response plan does not yet exist.
- **D2-1. Cyber Security Mindset**: There is minimal recognition of a cybersecurity mindset within government agencies. A leading ministry, KOMINFO, has begun to place priority on information security by identifying

risks and threats through the Information Security Index (KAMI Index). In the case of society at large, initial efforts have been made to make society aware of cyber threats through socialisation programs, but limited proactive steps exist to improve their cyber mindsets.

- **D2-2. Cyber Security Awareness:** Awareness-raising campaigns are established with a defined target, but different government organisations, such as the Directorate of Information Security (DITKAMINFO), ID-SIRTII, and Indonesian National Crypto Agency (LEMSANEG) conduct the awareness programme without coordination. There is no central online portal linking to the raising of cyber awareness, and a national cyber awareness campaign is limited, with very little cyber awareness material publicly available.
- **D2-3. Confidence and trust on the Internet:** There is an increased use of online services in Indonesia, such as e-government and e-commerce. Hence, trust in online services, in general, is considered as a legal and technical requirement. Initial efforts to provide more secure online services are being actively implemented, such promoting the use of National Root CA and the socialisation of the domain name, anything dot Indonesia, such as dot id (.id). In most cases, the government regulation No. 82/2012 covers those issues of trust in online services, as the government regulations for e-government and e-commerce services are under development.
- **D2-4. Privacy Online:** The government has started regulating access to personal data collected and stored across government agencies, public institutions, or electronic system operators. However, only minimal efforts have been made to develop a law on data protection or data privacy, as it is not currently under the National Legislation Program (Prolegnas) period of 2016. Additionally, as an important component of cybersecurity capacity factors, privacy in the workplace is currently not well-recognised and only limited efforts are made to provide a minimum level of privacy for employees.

- **D3-1. National availability of cyber education and training**: Minimal educational programmes in cybersecurity exist. Some major universities, such as Bandung Institute of Technology (ITB) and the University of Indonesia (UI) offer a master's degree in electrical engineering in cybersecurity courses, but there is no accreditation in cybersecurity education exists, and it is an ad-hoc education programme in the field of cybersecurity in Indonesia, as there is no national budget to support the cybersecurity capacity programmes.
- **D3-2. National development of cyber security education**: There are few professional instructors in cybersecurity, as no formal programme exists to train instructors or trainers in cybersecurity, because a budget justification for education and research does not exist.
- **D3-3. Training and educational initiatives within the public and private sector:** Few trained IT personnel are designated to support cybersecurity training programmes. Knowledge transfer from trained cybersecurity employees exists on an ad hoc basis.
- **D3-4. Corporate Governance, Knowledge, and Standards:** Some boards have some awareness of cybersecurity issues, and they have a general understanding of how companies are at risk.
- **D4-1. Cybersecurity legal frameworks**: Legislation and legal frameworks relating to ICT Security have been implemented. Legislation protecting the rights of individuals and organisations in the digital environment has been adopted. Privacy and data protection legislation does not exist, but partial legislation exists regarding privacy, data protection, and freedom of expression, such as Law No. 11/2008 and the Government Regulation No. 82/2012. Regarding substantive cybercrime law, Indonesia has adopted international instruments on cybercrime into the ITE law No. 11/2008.
- **D4-2. Legal Investigation**: The capacity of law enforcement authorities to prevent and combat computer-related crimes exists. Some capabilities to investigate and manage cybercrime cases have been established, such as digital forensic laboratories within POLRI and KOMINFO. This capacity is

meant to investigate computer-related crime, in accordance with the law No. 11/2008. Resources are dedicated to the operational cybercrime unit within POLRI and the Division of investigation and law enforcement within DITKAMINFO - KOMINFO.

- **D4-3. Responsible Disclosure:** Such a vulnerability disclosure provision is in place, in accordance with the government regulation No. 82/2012, but it is limited and only related to the protection of personal data. In the case of information disclosure related personal data, the public and private sector entities are required to report any information related to hacking or cyber-attacks, in which personal data is compromised.
- **D5-1. Adherence to standards:** Information security standards have been identified for use, such as ISO/IEC 27001. There have been some initial signs of promotion and adoption within the government agencies, public sectors, and critical national infrastructure organisations. In the case of the adoption of cybersecurity standards, there is a minimal implementation of SNI ISO/IEC 27001 or ISO/IEC 27001 on Information Security Management System in Indonesia (ISMS).
- **D5-2. National Infrastructure Resilience:** State-owned companies, such as PT Telkom, provide and manage national communication infrastructure. The government has minimal control of its own infrastructure, network, and system that are outsourced to external service providers. In most cases, there is a dependence on other countries for cybersecurity technologies.
- **D5-3. Cyber security marketplace:** No cybersecurity technologies are produced domestically. In most cases, foreign providers produce cybersecurity technologies and solutions, and those are widely used in the government agencies and private sectors.

The authors identify the following Top 20 recommendations for Indonesian Governments:

- **Recommendation #1:** Develop a national cybersecurity strategy (NCSS)
- **Recommendation #2:** Strengthen the role and coordination function of ID-SIRTII/CC as a national CERT.
- **Recommendation #3:** Create a formal list of CNIs on multi-stakeholder consultation and work with the companies that own and manage CNIs.
- **Recommendation #4:** Conduct crisis management exercises at a national level by inviting the relevant key national stakeholders, in order to ensure preparations for national cyber incident responses are well managed and robust.
- **Recommendation #5:** Create and build a dedicated civilian and military capability to help ensure that Indonesia has the capability to protect national interests in cyberspace.
- **Recommendation #6:** Establish emergency response asset priorities, in the event a service failure occurs, that aim at reducing impact.
- **Recommendation #7:** Develop a cybersecurity communication strategy to strengthen and expand the national cybersecurity campaign.
- **Recommendation #8:** Develop a single authoritative online portal for cyber awareness-raising amongst government agencies, businesses, and civil society across the country.
- **Recommendation #9:** Promote greater levels of trust in online services, such as e-government and e-commerce services.
- **Recommendation #10:** Develop a standard marketing strategy to promote privacy online for protecting personal data.
- **Recommendation #11:** Identify a centre of excellence in cybersecurity research and education to locate strengths and provide focused investment to address gaps.
- **Recommendation #12:** Promote cybersecurity training and education programmes designed for all employees at all levels of government

organisations, state-owned enterprises, private critical infrastructure providers, and small-medium enterprises.

- **Recommendation #13:** Create a national level register for information assurance and cyber security experts across the public and private sector as a way of bringing new talent into the profession.
- **Recommendation #14:** Raise awareness amongst senior government officials and board members of the critical national infrastructure operators concerning the cyber risks and actions they can take to protect security-sensitive information.
- **Recommendation #15:** Review existing legislation, for example, amending the ITE law No. 11/2008, to ensure that it remains relevant and effective in fighting cybercrime.
- **Recommendation #16:** Strengthen law enforcement and prosecutors' capabilities to investigate cybercrime and bring those responsible to justice.
- **Recommendation #17:** Create a single reporting system for electronic system operators for public services to report and disclose cybercrime incidents and data breaches, so that action can be taken.
- **Recommendation #18:** Promote cybersecurity requirements in government procurement processes for managing the national cyber defence.
- **Recommendation #19:** Establish a government unit under the related ministry to formally monitor and control national infrastructure, to help ensure Indonesia's security and resilience.
- **Recommendation #20:** Provide incentive-based cybersecurity solutions for local cybersecurity products or cyber insurance marketplace.

1 Introduction

1.1 Background

The current situation underlines the imperative for Indonesia to have a cybersecurity policy and strategy in place. The cyber policy and strategy should be based on the state's national interest. As stated in the preamble of the 1945 Constitution of the Republic of Indonesia, Indonesia's national aspirations aim to protect all the people of Indonesia and the entire homeland of Indonesia, to advance general prosperity, to develop the nation's intellectual life, and to contribute to the implementation of a world order[1]. Moreover, these objectives are reinforced by the Law No. 3/2002 on state defence, which aims to protect state sovereignty, national territory, and the nation's safety against all types of threats[2].

Indonesia is an interesting case study as a large emerging economy, with a GDP of around US$753.99bn. The number of Internet users online is increasing rapidly. According to the Indonesian Internet Service Provider Association (APJII), the number of Internet users will grow from 88.1 million in 2014 to 139 million by 2015[3]. PT Telkom is Indonesia's largest telecommunications company, with 9.52 million fixed-wire-line customers, 28.69 million fixed-wireless customers, and 137.37 million cellular customers as of June 2014. The government of Indonesia retains over 50 percent ownership of PT Telkom[4]. Indonesia has also one of the largest communities of Facebook users and Twitter account holders in the world[5]. ICT growth in Indonesia, and Indonesia entering the ASEAN Economic Community, will lead to a

[1] Nugraha et al. Towards Data Sovereignty in Cyberspace, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2610314

[2] Nugraha et al. An Adaptive Wideband Delphi Method to Study State Cyber-Defence Requirements http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2548249

[3] Asosiasi Penyelenggara Jasa Internet Indonesia. Penguna internet indonesia tahun *2014, http://www.apjii.or.id/v2/read/content/info-terkini/301/pengguna-internet-indonesia-tahun-2014-sebanyak-88.html*

[4] Nugraha et al, *supra* note 2

[5] BBCNews, http://www.bbc.co.uk/news/world-asia-17054056

proliferation of cross-border communication, and Indonesia will grow increasingly vulnerable to cyber threats. It was reported that Indonesia overtook China as the number one source of cyber-attacks in the second quarter of 2013[6].

The UK has world-class expertise in cybersecurity that can provide Indonesia with the vital skills needed in a rapidly evolving industry. The UK has an interest in making Indonesia's cyber environment secure, in order to provide UK's investors security when doing business in Indonesia.

1.2 Objective

To use the University of Oxford's Global Cyber Security Capacity Centre (GCSCC) Capability Maturity Model (CMM) in conjunction with the Indonesian Ministry of Communication and Information Technology (MICT) to develop a coherent national strategy for cyber policy, as driven by the CMM results. The study aims to help the Government of Indonesia develop a comprehensive policy and strategy on cybersecurity, currently absent from the cybersecurity landscape.

1.3 Methodology

The authors conducted a document analysis on policy and practice documents, and focus group consultations based on the CMM. It consists of five distinct areas of cybersecurity capacity; a) policy and strategy; b) culture and society; c) education, training, and skills; d) legal and regulatory frameworks; e) standards, organisations, and technologies. There are multiple factors in each dimension, which describe cybersecurity capacity. The factors that comprise each one of the dimensions are presented in *Table 1* below:

[6] Warwick Ashford, http://www.computerweekly.com/news/2240207541/China-no-longer-top-source-of-cyber-attacks

Table 1: Description of Factors within Each Dimension

Dimension	Factors in Each Dimension
Dimension 1 Policy and Strategy	D1-1: Documented or Official National Cybersecurity Strategy
	D1-2: Incident Response
	D1-3: Critical National Infrastructure (CNI) Protection
	D1-4: Crisis Management
	D1-5: Cyber Defence Consideration
	D1-6: Digital Redundancy
Dimension 2 Culture and Society	D2-1: Cybersecurity Mindset
	D2-2: Cybersecurity Awareness
	D2-3: Confidence and Trust on the Internet
	D2-4: Privacy Online
Dimension 3 Education, Training and Skills	D3-1: National Availability of Cyber Education and Training
	D3-2: National Development of Cyber Security Education
	D3-3: Training and Educational Initiatives within the Public and Private Sector
	D3-4: Corporate Governance, Knowledge and Standards
Dimension 4 Legal and Regulatory Frameworks	D4-1: Cybersecurity Legal Frameworks
	D4-2: Legal Investigation
	D4-3: Responsible Reporting
Dimension 5 Standards, organisations, and technologies	D5-1: Adherence to Standards
	D5-2: National Infrastructure Resilience
	D5-3: Cybersecurity Marketplace

Each factor includes indicators with five levels of capacity maturity, whereby the *initial* stage implies a rather ad-hoc level of capacity, and the highest stage describes both a strategic approach and an ability to dynamically adapt or change following environmental considerations. They are the following:

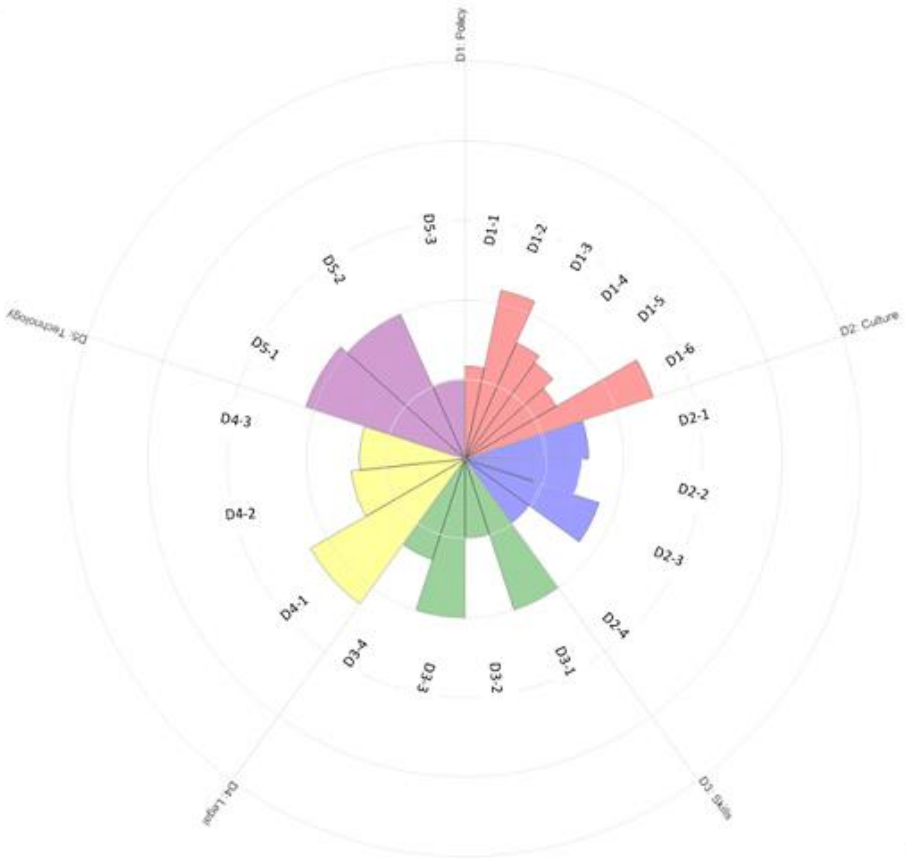
- **Start-up:** At this level, either no cybersecurity maturity exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.
- **Formative:** Some features of the indicators have begun to envolve and be formulated, but may be ad-hoc, disorganised, poorly defined, or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the sub-factor are in place and working. There is not, however, a well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the ‘’relative’’ investment in the various elements of the sub-factor. However, the indicator is functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important, for the particular organisation or nation. One thing cannot be as important as everything else, due to finite resources. Therefore, certain choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation's or organisation's particular circumstances.
- **Dynamic:** At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances; for example, the technology of the threat environment during a global conflict undergoes a significant change in one area of concern (e.g., Cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride, in a "sense-and-respond" manner. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are a feature of this level.

The following report serves as a review of the findings discussed during the cybersecurity capacity review in the Republic of Indonesia, and provides a set of recommendations on how the country might proceed.

Figure 1 below presents the maturity level for each dimension. The stages of maturity for each factor are represented by individual circles emanating from the middle of the graph, while each bar represents a single capacity factor, and each dimension is a fifth of the chart.

As seen in the graph, most factors of cybersecurity capacity in Indonesia lie between an *initial and formative stage* of maturity. However, there are only a few particular stages that are approaching the established stage, as only a few criteria have yet to be met.

Figure 1: CMM Review Results per Factor



1.4 Target Audience

The primary audience for this white paper is Indonesian stakeholders that have responsibility for, or an interest in, cybersecurity. Beneficiaries include policy makers, law enforcement, critical infrastructure owners, private sectors, incident response teams, national security and resilience organisations, academia, public administration organisations, and international organisations.

1.5 How to read this White Paper

This white paper aims to provide a basis for the Government of Indonesia to develop the country's national cybersecurity capacity, as follows:

I. **Section 2: Cybersecurity Policy and Strategy**

D1-1: Documented or Official National Cyber Security Strategy
This cybersecurity capacity factor covers a comprehensive national cybersecurity strategy that ties together different agencies and industries affected by cybersecurity into a coordinated and cohesive framework. This strategy often includes several areas and identifies roles and responsibilities of various actors engaging with cybersecurity.

D1-2: Incident Response
This cybersecurity capacity factor recognises that not all cyber incidents can be mitigated, so identifying which of these events constitute national-level threats can help narrow the scope of responsibility. Also, an organised and coordinated approach to incident response ensures that threats can be dealt with in the most efficient way possible.

D1-3: Critical National Infrastructure (CNI) Protection

This cybersecurity factor recognises that different governments may identify different entities as “critical infrastructure”, so it is important that the proper steps are taken to provide the cybersecurity necessary to protect these crucial assets. These steps should be based on careful planning and appropriate risk management.

D1-4: Crisis Management

This cybersecurity factor recognises that crisis management is more than incident response. Cyber exercises, for example, can simulate a variety of roles, from attackers to defenders, communications teams, coordinating bodies, and several others, all of which are crucial in the event of an actual crisis. Planning and evaluating crisis management applications provides stakeholders with the capacity to deal with real world scenarios.

D1-5: Cyber Defence Consideration

This factor identifies cyber defence considerations. There may be certain national security interests that Defence ministries and agencies are best positioned to engage with. Therefore, preparing a strategy for such action, with coordination between all organisations involved, is needed to ensure an integrated approach to confronting these threats to national security.

D1-6: Digital Redundancy

This capacity factor considers digital redundancy as a necessary element for cyber capacity. In the scenario where communication by electronic means is disabled, building back-up coordination links between emergency responders that do not rely on digital communications networks is crucial for enhancing cyber policy and strategy.

II. Section 3: Cyber Culture and Society

D2-1: Cyber Security Mindset

This cybersecurity capacity factor discusses aspects such as values, attitudes, and practices, including habits of individual users, experts, and other actors in the cybersecurity ecosystem. While a variety of actors need to have a cybersecurity mindset, including the government, private sector, and experts, it is also important to take into consideration socioeconomic aspects that contribute to different perceptions of cybersecurity.

D2-2: Cyber security Awareness

This cybersecurity capacity factor presents the need for programmes to raise cyber security awareness, with special emphasis on the perception of cyber risks and threats.

D2-3: Confidence and trust on the Internet

This factor presents aspects such as trust in the use of online services; trust in e-government and trust in e-commerce. Individuals' level of trust in using the Internet determines the extent to which they will provide personal information online.

D2-4: Privacy online

This factor discusses issues such as privacy and freedom of expression online. Specifically, privacy issues include the sharing of personal data in the public and private sectors, with emphasis on employee privacy. Freedom of expression, on the other hand, discusses the different perspectives and the diversity of actors and strategies that support freedom of expression online.

III. Section 4: Cybersecurity Education, Training, and Skills

D3 - 1: National availability of cyber education and training

This factor examines the country's resources/funding dedicated to increasing the availability of cybersecurity education and training. This availability needs to reflect the needs in the active cybersecurity environment.

D3 - 2: National development of cybersecurity education

This capacity factor discusses the importance of cybersecurity education development. The existence of cybersecurity education programmes, high-quality university and further education degrees and courses on cybersecurity, and the establishment of national and international cyber centres of excellence are measured in this factor.

D3 - 3: Training and educational initiatives within the public and private sectors

This cybersecurity factor discusses the development of training and educational initiatives within the public and private sectors. Cybersecurity training programmes can enhance employees' skillsets so that they have the ability to support cybersecurity issues as they occur. Cyber security knowledge exchange can also promote a continuous skill development.

D3-4: Corporate Governance, Knowledge, and Standards

This cybersecurity factor identifies corporate governance, knowledge, and standards that refer to private and state-owned companies' understanding of cybersecurity. The fact that boards need to have an understanding of the risks that companies face, some of the primary methods of attack, and how their company deals with cyber issues, are measured in this factor.

IV. Section 5: Legal and Regulatory Frameworks

D4-1: Cybersecurity legal frameworks

This cybersecurity factor seeks to encourage governments to enable the development of a secure Internet and online environment using sufficient, but not superfluous, law and regulation. This includes legal frameworks on ICTs, privacy, human rights, and data protection, and both substantive and procedural cybercrime law.

D4-2: Legal Investigation

This cybersecurity factor recognises that effective implementation of legal and regulatory frameworks through investigative tools are important in improving cybersecurity capacity. Law enforcement, prosecutors, and court officials need the appropriate investigative capacity to combat cyber-crime, including how to assess, obtain, and handle digital evidence, and utilise appropriate procedural instruments.

D4-3: Responsible Reporting

This cybersecurity capacity factor recognises that a responsible disclosure in place can provide specific guidelines and statements addressing how a vulnerability will be disclosed, and can enhance security capacity by repairing the vulnerability and preventing any future damage. This factor refers to a vulnerability disclosure model or reporting methodology, where a party (reporter) privately discloses information relating to a discovered vulnerability to a product vendor or service provider (affected party), and allows the affected party time to investigate the claim, and identify and test a remedy or resource, before coordinating the release of a public disclosure of the vulnerability with the reporter.

V. Section 6: Standard, Organization, and Technologies

D5-1: Adherence to standards

This cybersecurity capacity factor discusses the issue of implementation of standards and minimal acceptable practices by the private and public sectors, as well as standards on procurement and software development.

D5-2: National Infrastructure Resilience

This cybersecurity capacity factor focuses on infrastructure technology and national infrastructure resilience. Infrastructure technology underpins daily life and ensures the country continues to function socially and economically. Government and private sectors are capable of protecting the information systems of the state and the operators of critical infrastructures to ensure better national resilience.

D5-3: Cyber security marketplace

This cybersecurity capacity factor discusses the issues of availability of network and information cybersecurity technologies and specialist support for deployment, as well as cyber insurance, as a way of protecting against losses occurring directly to the insurance holder or against losses from another organisation or individuals affected by a security breach.

VI. Section 7: The Future of Cybersecurity Capacity in Indonesia

This section discusses opportunities, threats, strengths, and weaknesses, and the report concludes with the top 20 recommendations towards achieving greater cybersecurity capacity in Indonesia.

2 Cybersecurity Policy and Strategy

This dimension explores the capacity of the government to design, produce, coordinate, and implement a cybersecurity strategy, as well as policies upholding the strategy. Not every government has a national-level cybersecurity policy and strategy, or a responsible body for cybersecurity, as a policy area is still evolving. However, the importance of designating an overarching government body for cybersecurity coordination, and having a national cybersecurity strategy and policy, cannot be overemphasised. International experience shows that those governments that do have a designated government body and cybersecurity strategy and policy in place can better cope and mitigate with cyber incidents and attacks.

2.1 National Cybersecurity Strategy

Cybersecurity policy and strategy are essential to mainstreaming cybersecurity agenda within the government, because they help prioritise cybersecurity against other important policy areas, determine areas of responsibility and mandate of different cybersecurity government actors, and direct allocation of resources to the emerging and existing cybersecurity issues and priority areas.

Facts at a Glance: National Cybersecurity Strategy

Cybersecurity can be defined in many ways. The Oxford English Dictionary defines Cybersecurity as "the state of being protected against the criminal or unauthorised use of electronic data, or the measures to achieve this."[7]

The U.S. National Initiative for Cybersecurity Education (NICE) defines Cybersecurity as ''The activity or process, ability or capability, or state whereby

[7] Definition of cybersecurity: http://www.oxforddictionaries.com/definition/english/cybersecurity

information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation.'' [8]

The U.N. International Telecommunications Union defines Cybersecurity [9] as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and the organisation's and user's assets. The organisation's and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation's and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

No national cybersecurity strategy exists in Indonesia, but some cybersecurity issues are initially covered by Ministerial Decree No.41/2007 on General Guideline for National ICT Governance[10] and Circulars of the Minister No.05/SE/M.Kominfo/07/2011 on the Implementation of Information Security Governance for Public Service Operators[11]. In 2012, the Indonesian government issued the Government Regulation on the Operation of Electronic Systems and Transactions Number 82 of 2012 to address issues of Cybersecurity, such as electronic system governance and security in the implementation of the electronic system, as stated in Chapter 6 and seven respectively [12].

1. **Coordinating Ministry for Political, Legal, and Security Affairs (POLHUKAM)** established the National Desk on Resilience and Cyber Security (*Desk Ketahanan dan Keamanan Informasi Cyber Nasional* (DK2ICN)) in 2014 (The Decision of the Minister No. 24/ 2014). The objective of this desk is to establish a National Cyber Agency[13].

[8] US-CERT, https://niccs.us-cert.gov/glossary#cybersecurity

[9] ITU, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[10] LIPI, http://pdii.lipi.go.id/wp-content/uploads/2011/08/DETIKNAS.-2007.-Pedoman-Umum-Tata-Kelola-Teknologi-Informasi-dan-Komunikasi-Nasional.-Versi-1.pdf

[11]KOMINFO,https://publikasi.kominfo.go.id/xmlui/bitstream/handle/54323613/119/Panduan%20Penerapan%20Tata%20Kelola%20KIPPP.pdf?sequence=1&isAllowed=y

[12]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

[13] Munawar Ahmad, http://www.slideshare.net/msyani/badan-cyber-nasional?related=2

2. **Ministry of Communications and Information Technology (KOMINFO)** established several organisations dealing with cyber security matters, as follows:
    - The Directorate of Information Security was established in 2011 through a Decree of the Minister No. 17/PER/M.KOMINFO/10/2010 on the Organization and Administration of the Ministry of Communications and Information Technology[14].
    - ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure) established in 2007 by the Ministerial Decree No. 26/PER/M.KOMINFO/5/2007 on Security in the use of Telecommunication Networks based on Internet Protocol.
    - GovCSIRT (Government Computer Security Incident Response Team) was established by Decree of the Director General of ICT Application No. 01/SK/DJAI/KOMINFO/01/2012.
3. **Indonesian National Police (POLRI):** Within the State Police of the Republic of Indonesia there is a Cybercrime Unit, but its capacity remains limited due to a lack of human resources[15].
4. **Ministry of Laws and Human Rights** appoints Civil Service Officials with the Government, whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions, Telecommunications, and Intellectual Property.

Start-up - Formative: There is currently no national cybersecurity strategy for managing national cybersecurity capacity building in Indonesia, but there has been some initial work done on developing a national cybersecurity master plan within MCIT. Interestingly, many of the participants focused on the need for an organisation or a ministry mandated with the responsibility for coordinating cybersecurity. Some government ministries that attended the review suggested that a National Cyber Agency should be established within the Coordinating Ministry of Political, Legal, and Security Affairs as this central body. This National Cyber Agency would have representation from the other various security-oriented ministries, which raised concerns among other participants that national attention focuses too much on the threat environment and not enough on the benefits that could be drawn from cybersecurity. MCIT, in its identification of IT concerns, should insure that the private sector is consulted, so that there is a business-friendly environment surrounding

[14]KIMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/203/t/peraturan+menteri+komunikasi+dan+informatika+nomor+17permkominfo102010+tanggal+28+oktober+2010
[15] POLRI, http://www.reskrimsus.metro.polri.go.id/struktur-organisasi/kasubditIV

cybersecurity when moving forward. To improve the maturity of a national strategy to the *formative* and established stage, there needs to be more multi-stakeholder collaboration in the establishment of the central organisation, as well as in the identification of cross-ministerial and sectoral cybersecurity roles and responsibilities. Additionally, whatever the central body manifests as, this institution should be responsible for coordinating the development of a comprehensive national cybersecurity strategy.

2.2 Incident Response

This sub-dimension speaks about the capacity of the government to identify and determine characteristics of national level incidents, events, or threats in a systemic way - preferably, through a central registry. It also assesses the government's capacity to organise and coordinate an incident response

Facts at a Glance: Incident Response

There is a wide variety of acronyms for incident response teams that exist around the world, as are listed below[16]:

Acronym	Definition
CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IRC	Incident Response Centre or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

[16] http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?

It is encouraged that each institution, or group of the institution, develops its own incident response team to deal with cybersecurity. In 2012, the Ministry of Communication and Information Technology (KOMINFO) had made a public consultation on a draft of ministerial decree on a guideline for the establishment of the formation security incident response team[17]. However, the Ministerial Decree has not been issued so far. There are several incident response teams existing in Indonesia.

Firstly, ID-CERT (Indonesia Computer Emergency Response Team), established in 1998, that is intended for public sector and works based on complaints[18].

Secondly, ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure), established in 2007 by the Ministerial Decree No. 26/PER/M.KOMINFO/5/2007 on Security in the use of Telecommunication Networks based on Internet Protocol[19].

Thirdly, an amendment to the ministerial decree has been made to set up ID-SIRTII as CC (Coordinating Centre) that works based on monitoring logs, and has the capability to provide digital evidence for law enforcement[20].

In 2010, ID-SIRTII helped launch the Academic CSIRT (Acad-CSIRT), established for the University, which focuses on the development of security in Indonesia, and currently has 40 member Academic CSIRT Universities, both State and Private[21].

In 2012, GovCSIRT (Government Computer Security Incident Response Team) was established by the Decree of the Director General of ICT Application No. 01/SK/DJAI/KOMINFO/01/2012[22]. GovCSIRT cooperates with ID-CERT and ID-SIRTII to work with a range of government stakeholders, in order to develop a security capability for monitoring, evaluation, and incident response. Membership is open for all government entities, and, in 2013, the membership comprised 161 central government agencies, 33 provincial government entities, and 497 local governments[23].

[17] KOMINFO, http://kominfo.go.id/index.php/content/detail/3140/Siaran+Pers+No.+84-Pih-KOMINFO-11-2012+tentang+Uji+Publik+RPM+Pedoman+Pembentukan+Tim+Penanganan+Insiden+Keamanan+Informasi+/0/siaran_pers#.VnmbG1IYF_A

[18] ID-CERT, www.cert.or.id

[19]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/444/t/peraturan+menteri+komunikasi+dan+informatika+nomor+26permkominfo52007+tanggal+4+mei+2007

[20] ID-SIRTII, http://www.idsirtii.or.id/halaman/tentang/dasar-hukum.html

[21] ACAD-CSIRT, http://www.acad-csirt.or.id/

[22] GovCSIRT, http://govcsirt.kominfo.go.id/tentang-idgovcert/profil/

[23] Yudhistira Nugraha, http://www.slideshare.net/YudhistiraNugraha1/government-cybersecurity-forum-kl-2013

Formative: ID-SIRTII is the entity identified as chiefly responsible for incident response in Indonesia. While this organisation has been in operation for some time, it still faces difficulties in national coordination, as the national importance of cybersecurity has not been elevated to all ministries at this point. ID-SIRTII, as well as ID-CERT, has regularly collected some statistics regarding incidents in the country, which it makes publicly available. While this information is deemed as useful, several participants did not know whether those organisations could cope with a national-level incident, or if they would know what such an incident would look like. There is currently an effort underway to established sectoral incident response teams, but coordination between ID-SIRTII and the private sectors is currently limited to reactive information dissemination. The same can be said for the relationship between the government CSIRT, ID-SIRTII, and ID-CERT. Enhanced coordination, a proactive security posture, and a centralised threat classification would enable Indonesia's incident response to elevate its maturity.

2.3 Critical National Infrastructure

This sub-dimension studies the government's capacity to identify CNI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CNI asset owners, and enable comprehensive general risk management practices, including CNI risk management.

Facts at a Glance: Critical National Infrastructure

Australia	"Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."[24]

[24] http://www.tisn.gov.au/Pages/Critical_infrastructure.aspx

United Kingdom	The UK's national infrastructure is defined by the Government as: “those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends”.[25]
United States	The U.S.’s critical infrastructure sectors compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[26]

The Indonesian Ministry of Defence (KEMHAN) introduced the initial list of critical national infrastructure (CNI) assets in 2013, in which the ministry published the Roadmap for National Cyber Defence Strategy, that initially identified a list of critical national infrastructures in Indonesia, categorised into thirteen sectors (p.40-41)[27], as follows:

1. Defence and Security
2. ICT Infrastructure
3. Sea-Land-Air Transportation System
4. Finance and Banking Institution
5. Strategic Research Institution
6. Central and Local Government Agencies
7. Infrastructure Control Systems and Energy
8. Education and Health Services
9. Water and Transportation Infrastructure
10. Citizen Information System
11. Trade and Industry
12. Art, Culture, and Tourism
13. Other Sectors based on emerging risks

Moreover, the Law No. 25/2009 on Public Service identifies strategic sectors in public services, including education, teaching, property, ICT, health, social insurance, banking, transportation, natural resources, and tourism[28].

[25] CPNI-UK, http://www.cpni.gov.uk/about/cni/
[26] DHS-US, http://www.dhs.gov/what-critical-infrastructure
[27] Cybersecuritynews, http://cybersecuritynews.id/2016/02/08/indonesias-roadmap-for-national-cyber-defence-strategy/
[28] POLHUKAM, http://upp.polkam.go.id/wp-content/uploads/2015/04/uu2009_025.pdf

Start-up - Formative: At a national level, no list of CNI assets has been formally defined, nor has a framework for collaboration between CNI owners been identified. Though the Ministry of Defence categorised 12 entities amongst the private and government sectors as composing critical national infrastructures (CNIs), this list was not generated to specifically consider cybersecurity strategy, and one participant said that the President has not yet passed the list of CNIs, so this list has not been disseminated more broadly. At this point, there is no organisation responsible for coordinating the relationship between CNIs and the government. Some participants felt this should be the role of ID-SIRTII or GovCSIRT, but there was no consensus on this. Additionally, it seems that IT implementation, rather than information infrastructure and cybersecurity, is the primary concern of CNIs at the moment. The degree to which cybersecurity is a concern depends largely on the type of organisation. Finally, many participants felt that regulation was required in order to enable genuine collaboration on cybersecurity response planning and risk management. While the government has government regulation No. 60/2008 and government regulation no. 82/2012, which lay out risk management requirements for public services, this has not yet been adopted in terms of cybersecurity.

2.4 Crisis Management

Crisis management planning and evaluation capacity, bolstered by functional protocols and standards, is critical to implementing cybersecurity policies that are results-oriented and sustainable. Crisis management planning usually entails, but is not limited to, the conduct of specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation, but would also inform budgetary allocations.

Facts at a Glance: Crisis Management

Cybersecurity exercises at the national level have not been formally conducted. However, ID-SIRTII annually conducts the Drill Test, called ''National Cyber Storm Drill Test'', staged as a national event. The drill test is only a drill to check whether governments, private companies, and other computer infrastructure could handle major cyber-attacks. The exercise is to examine whether those stakeholders affected by cyber-attacks can communicate with each other and coordinate among themselves to minimise damage and perhaps block the spread of the attacks. The list of players includes government agencies, information technology representatives from banking and finance, the chemical industry, major telecom firms, the energy sector, defence contractors, and those from the transportation, atomic energy, and other utility infrastructures.[29] ID-SIRTII also regularly conducts a competition-based Drill Test, called ''The Amazing Trace''. The amazing trace is a competition of skills from various tough teams in detecting, preventing, and combating cybercrime[30].

Indonesia has become a full member of the AP-CERT through the membership of ID-SIRTII and ID-CERT[31]. Indonesia, through the membership of ID-SIRTII/CC, has become a full member of the Forum of Incident Response and Security Teams (FIRST)[32], as well as a full member of the Organisation of the Islamic Conference-CERT (OIC-CERT)[33]. Those memberships provide a platform for their members to develop collaborative and effective approaches to cybersecurity incidents, as well as to improve the region's awareness and competency in relation to cybersecurity incidents.

Start-up - Formative: There is some understanding that cybersecurity exercises against national cyber incidents are necessary for national security. Crisis management exercises and simulations in Indonesia are currently focused on incident response and IT security professionals rather than policy-makers. Through ID-SIRTII, the cyber exercises are being conducted based on competition against specific cyber-attacks. However, results from exercises do not inform overall crisis management at a national level. Moreover, Index KAMI is a tool designed by MCIT meant to help identify cyber readiness of different government entities, but this tool has only been implemented in certain government ministries and local governments.

[29] ID-SIRTII, http://www.idsirtii.or.id/ncsd/arsip/2013.html
[30] ID-SIRTII, http://tat.idsirtii.or.id/#explore
[31] APCERT, http://www.apcert.org/about/structure/members.html
[32] FIRST, https://www.first.org/members/teams
[33] OIC-CERT, http://www.oic-cert.org/en/fullmembers.html#.VnrtNFIYF_A

Additionally, the Organisation of the Islamic Cooperation CERT (OIC-CERT) and Asia-Pacific CERT (AP-CERT) have hosted some semi-annual exercises, online and in-person, during the regular meetings in order to raise the capacity of ministry security professionals. There is also some evaluation of results, although the applicability of the feedback has been questioned due to the legal differences between countries. These exercises and competitions also help map potential capacity vulnerabilities, according to the participants. However, there are no multi-stakeholder exercises conducted, nor is there a policy-maker representation in such exercises. Including such participants would elevate the country's maturity in crisis management.

2.5 Cyber Defence Consideration

This sub-dimension explores whether the government can design and implement a cyber-defence strategy and lead its implementation, including through a designated cyber defence organisation within the executive branch. Among others, it also assesses the level of coordination between various public and private sector actors in response to malicious attacks on military information systems and critical national infrastructure.

Facts at a Glance: Cyber Defence Consideration

The past five years have seen a number of cyber defence initiatives in Indonesia, posed by the Indonesian Ministry of Defence (MoD), as follows:

- Cyber Defence Consideration is covered by the Decision of the Minister of Defence No. 25/2014 on State Defence Policy 2014[34][35].
- The government issued the Defence Ministerial Decree No. 38/2011 on Cyber Defence Information Systems Policy[36].
- The MoD developed a Roadmap for National Cyber Defence Strategy[37].

[34] KEMHAN, http://dmc.kemhan.go.id/images/uploads/291572KepJakhaneg2014.pdf
[35] KEMHAN, http://dmc.kemhan.go.id/images/uploads/800113Jakhanneg-2014.pdf
[36] KEMHAN, http://www.kemhan.go.id/kemhan/files/e9eee96ac85c48bf766886fbef1afd8b.pdf
[37] CybersecurityNews, http://cybersecuritynews.id/2016/02/08/indonesias-roadmap-for-national-cyber-defence-strategy/

- Bilaterally, Indonesia co-operates and signed a Memorandum of Understanding (MoU) with Japan to strengthen defence capabilities such as cyber defence[38].
- The government issued the Defence Ministerial Decree No. 68/2014 on Information Security within the Indonesian MoD and Indonesian National Army[39].

Start-up - Formative: A roadmap for national cyber defence strategy exists. However, according to the participants, cybersecurity defence is still a *start-up* in terms of its strategic cybersecurity approach. The Ministry of Defence lacks human resources to organise itself toward more profound cyber defence. There is also limited coordination between defence organisations and the broader community of actors; the approach to national cyber defence remains isolated to each sector or ministry at this point. Moreover, minimal security standards and controls have been carried out in government procurement of products and services, but it is still a limited effort. Improving organisation and cooperation in this area is key to improving maturity.

2.6 Digital Redundancy

Digital redundancy foresees a design of a cybersecurity system in which the proper backup safeguards duplication and failure of any component. This sub-dimension assesses the government's capacity to plan and organise redundancy communication among stakeholders.

Facts at a Glance: Digital Redundancy

Article 16, the Government Regulation No 82/2012[40] states that Electronic System Operators for Public Service shall apply good and accountable governance, such as availability of a plan for the sustainable Electronic System Operation that it manages.

[38] KEMLU, http://treaty.kemlu.go.id/uploads-pub/5696_JPN-2015-0513.pdf
[39] KEMHAN, http://www.kemhan.go.id/kemhan/files/016a206e6c1d746ea38d6bbbf251cfe1.pdf
[40]https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

Article 17 also states that Electronic System Operators for Public Service shall have a business continuity plan to cope with disturbance or disaster in relation to the risks of the impact that may arise.

What it means by ‘’business continuity plan’’ is a series of processes performed to ensure continuity of activity when there are disturbances or disasters.

Formative - Established: There is digital redundancy capacity within government and law enforcement in Indonesia, as business continuity plans and a disaster recovery centre are security requirements stated in regulation. Those redundancy efforts are some of its more advanced cybersecurity capacities. There are business continuity plans in place in the event of a disruption, and several ministries conduct simulations and drills that help them determine critical data. Redundant communication channels in the network infrastructure are in place, provided by PT Telkom. There is also a data centre to backup information, but this is not automated. Additionally, ID-SIRTII has been identified as having a contingency plan in the event of a major incident, but these plans have not yet been tested. Mapping out the redundancy efforts in the network infrastructure would greatly benefit capacity in this area.

2.7 Conclusion

The six factors of capacity in policy and strategy in Indonesia range in maturity between the *start-up* and *formative* stages, with some factors on their way to the established stage; none, however, have fully achieved this stage.

- **National Cyber Security Strategy**: There is no evidence that a cybersecurity strategy exists in Indonesia. However, discussion processes through the Desk on Cyber Security have been established for key stakeholder groups. Some government organisations, such as POLHUKAM, KOMINFO, LEMSANEG, KEMHAN, and POLRI, deal with cybersecurity components. A variety of cyber programmes have been designated within each government entity. However, no formal focal point exists for cybersecurity coordination in Indonesia. Budgets related to cybersecurity exist, but they reside in the disparate

department or government ministries. While budgets exist in the different department, such as the Directorate of Information Security and ID-SIRTII, inter-departmental cooperation and coordination are still limited for a coordinated cyber programme. Some national strategies may exist in relation to cybersecurity, but it is not necessarily aligned with national goals, and does not provide actionable directives for cybersecurity capacity development in Indonesia.

- **Incident Response**: Certain cyber threats have been categorised, but they are not formally identified and recorded as national level incidents. Formal coordination or information sharing mechanisms established within government entities are limited through Gov-CSIRT. Even though ID-SIRTII is considered as CC (Coordinating Centre), the national incident response is limited and the response is still reactive. Co-ordinated national incident response is established through ID-SIRTII, but lines of communication remain ad hoc for crisis situations.
- **Critical National Infrastructure (CNI)**: The Ministry of Defence created a general list of CNI assets through the Roadmap for National Cyber Defence Strategy in 2013, but it was done without identified risk-based priorities. Moreover, there is little evidence of interaction between government ministries and owners of critical assets. A formal collaboration mechanism is under development by the Directorate of Information Security. Some formal plan may exist in some critical national infrastructures, such as information protection procedures and processes. However, response planning to an attack on critical assets has been discussed with limited cyber security capability solutions. Such discussions within Indonesian National ICT Council and Ministry of Defence have occurred to determine which industries and bodies are critical to the national cyber ecosystem. However, there is a lack of regular dialogue between tactical and executive strategic levels regarding cyber risks against critical assets. Moreover, cybersecurity requirements and vulnerabilities in CNIs have not yet been identified. However, some

vulnerability review processes have been implemented for compliance purposes. Some awareness and training have been provided so that incident management within the CNI can be applied efficiently. Security measures and guideline for CNIs are under development by adopting SNI ISO/IEC 27001. Monitoring and review processes of the implementation of CNI standards are also under development by the Directorate of Information Security.

- **Crisis Management**: Minimal crisis management or drill test in cybersecurity based on competition has been undertaken by ID-SIRTII within a simple exercise scenario of attack. Some key stakeholders are involved in the drill test, which is regularly conducted by ID-SIRTII. Participants, on an ad-hoc basis, evaluate the exercise, but it does not feed into the decision-making process. Results for cyber exercises do not inform overall crisis management at a national level.
- **Cyber Defence Consideration**: A national cyber defence strategy exists, outlining specific threats to national security in cyberspace, such as state-sponsored attacks and threats to defence and military operational capacity. However, a coordinated response strategy does not yet exist in practice. Thus, there is no clear command structure for cybersecurity in the Indonesian armed forces. In the case of cyber defence operation, the Ministry of Defence is responsible for defence during conflict using cyber means, in cooperation with KOMINFO and ID-SIRTII. The Indonesian armed forces have a limited capacity for cyber resilience, intended to reduce vulnerabilities in the national infrastructure. This is because there are no formal cyber defence capability requirements agreed upon between the public and private sectors to minimise cyber threats against national security.
- **Digital Redundancy**: Digital redundancy measures are considered as cybersecurity requirements, especially for public services. In most cases, standard operating procedures are established in the event of a communication disruption. However, a national cyber emergency response plan does not yet exist.

3 Cyber Culture and Society

This dimension assesses essential elements of a responsible cyber-culture at the individual and organisational levels, as perceived by a variety of stakeholders. Aspects of a cyber-culture include the level of trust in Internet services, such as in e-government and e-commerce, and adherence to standards of privacy in handling personal information by all entities engaging in the provision of these services. All cybersecurity experts need to avoid blaming users for problems with cybersecurity. However, experts need to build systems and programmes to ensure that users are aware of threats, know how to incorporate good practices, and help incorporate these practices into their routine behaviour online.

3.1 Cybersecurity Mindset

This sub-dimension evaluates the level of recognition and priority attached to the cybersecurity mindset by the government, private sector, and society at large. Cybersecurity mindset is understood as a predisposition and, in particular cases, as a consistent behavioural model toward alignment of one's actions with cybersecurity priorities on an individual level or in an organisational setting. A cybersecurity mindset consists of values, attitudes, and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem.

Facts at a Glance: Cybersecurity Mindset

There is increasing awareness of cyber risks within government entities in relation to the Circulars of the Minister No.05/SE/M.Kominfo/07/2011 on the Implementation of Information Security Governance for Public Service Operators[41].

The Information Security Index, also known as the KAMI index, is a framework for assessing domestic information security across government entities, in both central

[41]KOMINFO,https://publikasi.kominfo.go.id/xmlui/bitstream/handle/54323613/119/Panduan%20Penerapan%20Tata%20Kelola%20KIPPP.pdf?sequence=1&isAllowed=y

and local government agencies. The areas of the KAMI Index include information security governance, risk management, framework, assets management, and technology and information security. In 2011-2014, 209 government entities, in both central and local government agencies, were evaluated using the KAMI Index[42].

The National Resilience Institute (LEMHANNAS), which aims to conduct education and training for senior Indonesian officials, recently held the International Conference on Cyber Security to consider cyber security as a priority attached to national development by the related stakeholders[43].

Start-up - Formative: There are only very initial steps being taken to adopt a cybersecurity mindset in Indonesia. The government, private sector, and civil society are equally under-aware of the threats posed by cybersecurity. Cyber risks and threats have begun to be identified through the assessment of Index KAMI across central and local government entities. Participants said this lack of mindset is primarily due to a lack of socialisation of cybersecurity issues across society. In government, a lack of a coordinating agency hinders the promotion of such a mindset, an issue which is heightened at the local level, where the proliferation of such a mindset is much more difficult. A report titled, “Meeting the cyber security challenge in Indonesia”, highlights the need for commitment from leaders in developing a cybersecurity strategy, which would then channel cybersecurity socialisation efforts across a broad group of stakeholders. In the private sector, telecommunications companies are usually at the forefront of cybersecurity awareness, but other companies seriously lag behind. Some leading firms, such as PT Telkom, PT Indosat, and PT Indonesia Stock Exchange, have obtained a certification of ISO/IEC 27001. Indeed, even some companies, required to implement ISO 27000 series security standards, cannot do so due to lack of awareness. Finally, in civil-society, there is still an ongoing effort to improve ICT literacy, so cybersecurity is lower in priority in relation to this effort.

[42] Annual Report 2014 – APTIKA, http://aptika.kominfo.go.id/unduh/LAPTAH%20Aptika%202014.pdf
[43] SETKAB, http://setkab.go.id/bicara-di-lemhanas-seskab-hanya-akan-ada-satu-lembaga-awasi-masalah-cyber/

3.2 Cybersecurity Awareness

This sub-dimension evaluates the need for programmes to raise cybersecurity awareness across government entities, businesses, and civil society, with particular emphasis on the perception of cyber risks and threats.

Facts at a Glance: Cybersecurity Awareness

Indonesia conducts the socialisation of cybersecurity across society-at-large. The Directorate of Information Security under the Division of Information Security Culture aims to establish an information security culture and promote information security awareness at a national level, in particular for government entities and society[44]. The Division of Culture has been conducting the socialisation of information security across the region since the Directorate of Information Security was established in 2011.

ID-SIRTII also conducts security awareness, including seminars and courses, across society, especially for young people and those that have good computer literacy [45].

LEMSANEG (National Cryptography Agency) also provides information security initiatives, such as seminar, called SKKI (Information Security Awareness Seminar), in particular for government entities[46].

On a global level, Indonesia works together with ASEAN-Japan to enhance security awareness across the region[47]. Also, it is worth noting that one of the main aspects of the ITU's Global Cybersecurity Agenda is to strengthen cybersecurity capacity through ITU-IMPACT (International Multilateral Partnership Against Cyber Threat) partnership. The IMPACT programmes-related cybersecurity are widely socialised across the ITU's member countries[48]. Moreover, ASEAN ICT Masterplan (AIM 2020) aims to promote cybersecurity cooperation, as well as strengthen cybersecurity capacity, among ASEAN countries[49]. All these ASEAN activities also promote cybersecurity awareness in Indonesia.

[44] Ditjen APTIKA, http://aptika.kominfo.go.id/index.php/profile/direktorat-keamanan-informasi
[45] IDSIRTII, http://idsirtii.or.id/kegiatan.html
[46] LEMSANEG, http://www.lemsaneg.go.id/?s=seminar
[47] NISC, http://www.nisc.go.jp/aj-sec/
[48] IMPACT, http://www.impact-alliance.org/countries/alphabetical-list.html
[49] ASEAN, http://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

Start up - Formative: Cybersecurity awareness across a national level remains limited. Some awareness campaigns concentrate on child online protection and content filtering at this point in time. The notion of a "healthy Internet" is often associated with preventing content that could potentially harm the moral fabric of society. Participants felt that MCIT has the responsibility for raising awareness for cybersecurity, and the participants identified the need for raising awareness in this area. Though some government organisations dealing with cyber awareness exist, there has not been a coordinated campaign on this front at this point, with other actors. Banks may have some inter-sectoral awareness efforts, but these are ad-hoc. The on-going implementation of cybersecurity awareness-raising within government entities, such as KOMINFO and LEMSANEG, does not necessarily cover all of the stakeholder groups at the national level. Moving the awareness-raising purview away from content filtering, and more toward genuine cybersecurity awareness-raising campaigns, would be a great benefit for this capacity.

3.3 Confidence and trust on the Internet

This sub-dimension assesses the level of stakeholders' trust in the use of online services, in general, and trust in e-government and e-commerce services, in particular.

Facts at a Glance: Confidence and trust on the Internet

Trust in the use of online services has been identified as a requirement in Indonesian laws, such as the Information and Electronic Transactions Law Number 11 of 2008[50], and the Government Regulation on the Operation of Electronic System and Transactions Number 82 of 2012[51].

E-Government services have been developed, starting with the Presidential Instruction No. 3/2003 concerning National Policy on E-Government

[50]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[51]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

Development.[52] Organisationally, KOMINFO, under the Directorate General (DG) of Information Technology's Application, deals with the trust in the use of e-government services. The latter is particularly relevant to e-government, as it is home to the Directorate of e-government under the DG of Information Technology's Application[53].

E-commerce services are partly covered by the Government Regulation on the Operation of Electronic System and Transactions Number 82 of 2012, and have not been fully developed. A draft of the Government Regulation on E-Commerce is under development[54].

Formative: The focus in discussions on trust in the use of online services was on e-government services and e-commerce services. Regarding trust in the use of e-government services, there was a general perception among the participants that the National Public Procurement Agency's (LKPP) National Procurement Portal (INAPROC) is provided in a secure way, but there is no evidence to support this assumption. The Director General of Tax (DGT) Online is Indonesia's online tax submission service and, given that there has not been a major incident in the provision of this service thus far, citizens seem to trust the security of this service. No organisation is responsible for improving trust in the provision of these services. E-commerce services are rapidly expanding in Indonesia, and accompanying legislation hopes to increase the trust in the use of these services. For example, there is a requirement that public-facing commerce platforms must register with MCIT, in hopes of reducing the number of fraudulent services. However, there was a question among participants as to whether this law is enforced. Security, according to the participants, is still not a primary concern for these providers, and some organisations, such as a few banks, have witnessed major security incidents that have reduced the trust in their services.

[52]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[53] KOMINFO, http://aptika.kominfo.go.id/index.php/profile/direktorat-e-government

[54] KEMENDAG, http://ditjenpdn.kemendag.go.id/id/berita/regulasi/naskah-akademik-rancangan-peraturan-pemerintah-rpp-tentang-perdagangan-elektronis-e-commerce

3.4 Privacy Online

This sub-dimension assesses the level of salience of privacy issues in the government agenda through the enactment of relevant practices, laws, and regulations, and the level of engagement and advocacy around them by civil society. It also evaluates how national legislative norms adhere to regionally and internationally recognised standards for human rights.

Facts at a Glance: Privacy Online

A discussion has begun on privacy issues through stakeholder engagement. The Information and Electronic Transactions Law Number 11 of 2008 in Article 26[55] has briefly covered the use of personal information online.

The Government Regulation on the Operation of Electronic System and Transactions Number 82 of 2012 in Article 15[56] are regulating access to personal data collected and stored across Electronic System Operators, but the provision of personal data or data privacy is limited. This provision requires an operator to maintain the secrecy, integrity, and availability of personal data that it manages. In particular, Operators must obtain user consent in the acquisition, usage, and utilisation of personal data. The data owner must approve data usage and disclosure.

To follow up the Government Regulation, the government has recently published a draft of the decree of the Minister on Personal Data Protection in Electronic System[57]. Moreover, the government is now working on the development of the Data Protection Act or the Data Privacy Act[5859].

Start-up: There is a major gap in cybersecurity capacity when it comes to privacy and data protection. At the moment, there is no discussion about the role of privacy

[55]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/167/t/undangundang+nomor+11+tahun+2008+tanggal+21+april++2008

[56]KOMINFO,https://jdih.kominfo.go.id/produk_hukum/view/id/6/t/peraturan+pemerintah+republik+indonesia+nomor+82+tahun+2012

[57] KOMINFO,http://kominfo.go.id/index.php/content/detail/5128/Siaran+Pers+No.53-PIH-KOMINFO-07-2015+tentang+Uji+Publik+Rancangan+Peraturan+Menteri+mengenai+Perlindungan+Data+Pribadi+dalam+Sistem+Elektronik/0/siaran_pers#.VoFNn9Corww

[58] KOMINFO,http://peraturan.go.id/proleg/detail/11e4e1836e5fec86828d303931383533.html

[59]KOMINFO,http://kominfo.go.id/index.php/content/detail/6142/Kemkominfo+Siapkan+RUU+Perlindungan+Data+Pribadi/0/sorotan_media#.VoFS09Corww

in the provision of cybersecurity in the country, which indicates that this issue is not a priority in the slightest. While the IT Law briefly mentions data protection, there is no other discussion about ensuring data protection at the national level or in the workplace. Other than classifying certain types of information, no organisation implements rules or guidelines for protecting the data of Indonesian citizens. This is important, because without appropriate data protection or privacy considerations there could potentially be a major backlash from domestic and international sources regarding inappropriate or inadequate protection of citizen information and rights. This issue should be taken more seriously moving forward.

3.5 Conclusion

The four factors of capacity in cyberculture and society in Indonesia ranges in maturity between the *start-up* and *formative* stages, with some factors on their way to the *established* stage; none, however, have fully achieved this stage.

- **Cyber Security Mindset**: There is minimal recognition of a cybersecurity mindset within government agencies. A leading ministry, KOMINFO, has begun to place priority on information security by identifying risks and threats through the Information Security Index (KAMI Index). The KAMI Index has been widely implemented across central and local government entities. Such cyber security standards, like SNI ISO/IEC 27001, are widely implemented and adopted across government and industry entities. In the case of society at large, efforts have been made to make society aware of the cyber threat, but with limited proactive steps to improve their cyber mindsets.
- **Cyber Security Awareness:** Awareness-raising campaigns are established with a defined target, but different government organisations, such as the Directorate of Information Security, ID-SIRTII, and National Crypto Agency, conduct the awareness programme alone. The Directorate of Information Security provides online resources, such as presentation slides and guidelines concerning information security, but with no measurement effort, and, in most

cases, online resources are distributed to the public through social media, like slideshare.com. There is no central online portal linking to cyber awareness-raising and a national awareness campaign is limited and publicly promoted.

- **Confidence and trust on the Internet:** There is an increased use of online services in Indonesia. Hence, trust in online services, in general, is considered as a legal and technical requirement. Efforts to provide more secure online services are implemented, such as the use of National Root CA. A Coordinated national programme to promote trust in online services has been partly implemented through the socialisation of domain name anything (.id). In the case of e-government services, KAMINFO has publicly promoted the necessary secure environment, such as the installation Private Network Security Box (PNSBox), across government agencies. In most cases, the range of e-government services continues to expand, with limited security measures to promote secure e-government services. In the case of e-commerce, users lack adequate knowledge of electronic commerce services, and e-commerce services are minimal and only partly established in a secure environment. The government regulations for e-government and e-commerce services are under development, but those issues are covered by the government regulation No. 82/2012.
- **Privacy Online:** The government regulates access to personal data collected and stored across government, public institutions, or electronic system operators. In particular, the discussion has begun to develop a law on data protection or data privacy. However, privacy in the workplace is not well recognised as an important component of cyber security, and only limited efforts have been made to provide a minimal level of privacy for employees.

4 Cybersecurity Education, Training, and Skills

This dimension assesses the availability and quality of cybersecurity education, training, and skills in Indonesia for various groups of government stakeholders, the private sector, and the population as a whole. In particular, it evaluates existing educational offerings and national development of cybersecurity education, training and educational initiatives within public and private sector, and corporate governance, knowledge, and standards.

4.1 National Availability of Cyber Education and Training

This sub-dimension speaks to the importance of the availability of high-quality cybersecurity education and training options, and their integration and synergies, to ensure an adequate and sustainable supply of cybersecurity skills for the needs of the public and private sectors. It takes stock of existing educational offerings in schools and universities, and training offerings within the private sector and beyond in the field of information security and cyber security, and provides a superficial evaluation of their structure and components.

Facts at a Glance: National Availability of Cyber Education and Training

In 2014, Bandung Institute of Technology (ITB) in cooperation with Korean International Cooperation Agency (KOICA) inaugurated ITB-Korea Cyber Security Research and Development Centre in Indonesia, which is Indonesia's first cyber security centre[60]. The Centre will host many activities to support cybersecurity education and research, especially for a security master's program and doctoral program.

[60] ITB, http://csc.stei.itb.ac.id/about/

Other universities also offer a similar master's program. Since 2013, the University of Indonesia, in cooperation with ID-SIRTII, offers a master's program in Information Network Security[61].

A variety of stakeholders are conducting training programs in cybersecurity, such as ISACA Indonesia Chapter, which cooperates with some local training providers[62], but the training programs are ad-hoc and uncoordinated with national priorities. ID-SIRTII also offers cybersecurity training, such as digital forensic and incident handling[63].

Formative: There are some courses in cybersecurity being offered at the university level. Some courses on cybersecurity, such as IT security, cryptography, network security, information assurance, and ethical and legal practice in information security, are offered by some universities within a number of bachelor's and master's degrees. For example, the Bandung Institute of Technology offers a master's degree in Engineering in Information Security, which includes tracks in either engineering or management[64]. ITB are seeking to implement security and privacy as a lecture in all computer science courses. Telkom University and the University of Indonesia also offer courses in cybersecurity at the bachelor's and master's levels, and Telkom University hopes to offer degree programmes similar to ITB in these areas in the near future. According to the focus group participants, universities are reaching out to local businesses to try to meet the needs of the industry. Also, the Defence Ministry has funds to build an Indonesian cyber centre, in order to build capacity and human resource on education and training in schools, but the development of the centre has been delayed. Moreover, various training programs in information security do take place, but it is rather ad-hoc and uncoordinated as a national program. At lower levels of education, however, students are primarily focused on the functionality of information technologies, rather than the security that enables these products. Several participants felt that there should be an effort to build awareness for the younger generation in a non-formal campaign for the safe use of gadgets.

[61] Universitas Indonesia, http://www.ui.ac.id/berita/menghadapi-tantangan-di-era-cybersecurity.html
[62] ISACA, http://www.isaca.org/chapters11/Indonesia/NewsandAnnouncements/Pages/default.aspx
[63] ID-SIRTII, http://www.idsirtii.or.id/kegiatan.html
[64] ITB, http://ip.stei.itb.ac.id/wp-content/uploads/2015/02/Brosur-International-Master-Program-SEEI-Ver.2015-04-07.pdf

Additionally, there is a need for the education ministry to work with universities to provide incentives for the promotion of cybersecurity education among all schools. Such cooperation between the Ministry of Education and universities would help enhance the scope, scale, and quality of the course offerings in cybersecurity. Hopefully, this will also increase the number of graduates in information and cybersecurity.

4.2 National Development of Cybersecurity Education

This sub-dimension explores what kind of incentive structure exists for the national development of cybersecurity education; for example, whether any education strategy for developing cybersecurity skills exists, whether cyber security as a discipline is given priority in educational curricula, and whether an adequate budget allocation is present.

Facts at a Glance: National Development of Cybersecurity Education

No national education strategy and educational curricula in cybersecurity exists, but some accredited and major universities, such ITB and UI, have a master's program in cybersecurity[65] [66]. In 2006, Indonesian Ministry of Education included Information and Communication Technology (ICT) as one of the subjects in the national education curricula, ranging from primary to senior high school. However, in 2013, the ICT subject is no longer part of the national curricula[67]. Later on, the Minister of Communications and Information Technology suggested to the Minister of National Education and Culture to include computer programming or coding as one of the subjects in national education, starting from the primary level[68].

Start-up: There is no incentive for training and education in cybersecurity, because state budgets for training, research, and development have not yet been allocated

[65] ITB's Cyber Security Centre, http://csc.stei.itb.ac.id/about/
[66] University of Indonesia, http://www.ui.ac.id/berita/menghadapi-tantangan-di-era-cybersecurity.html
[67] Change.org, https://www.change.org/p/mendikbud-m-nuh-jangan-hapus-matpel-tik-kkpi-di-kurikulum-2013-mata-pelajaran-teknologi-informasi-dan-komunikasi-tik-di-sd-smp-sma-dan-kkpi-di-smk-harus-ada-dalam-kurikulum-sekolah
[68] KOMINFO, http://kominfo.go.id/index.php/content/detail/5875/Menkominfo-membuka-acara-Robotic-Day-2015/0/berita_satker#.VqfXq9Corww

specifically for cybersecurity education. The Ministry of Education had placed the ICT subject as part of the curricula for all levels, ranging from primary to high school, but it is no longer available. Moreover, the Indonesian National ICT Council has placed the national broadband program as a priority. This will be considered in the efforts to build cybersecurity initiatives in Indonesia.

4.3 Training and Educational Initiatives within the Public and Private Sectors

This sub-dimension assesses the scope of horizontal and vertical cybersecurity knowledge transfer within organisations, and how it translates to continuous skill development. Apart from the question of strategic staffing, cybersecurity is a highly technical specialised field, and, therefore, strategic development and deployment of skillsets and tools to support them is central to maintaining organisations secure and mainstreaming cybersecurity culture within organisational structures.

Facts at a Glance: Training and Educational Initiatives

KOMINFO has two ICT Training Centres, which were developed in cooperation with KOICA. BPRTIK (ICT Training and Development Centre) is intended for the private sectors and society[69]. BPRTIK (National ICT Research and Training Centre) is intended for the public sector[70]. Those agencies offer training for the National Working Competency Standards (SKKNI) in the following area: Network Administrator, Programmer, Technical Support, and Web Programmer[71][72].

The ICT Research and Human Resource Development, KOMINFO, is currently working on the development of ASEAN ICT Skill Standards, such as Software Development, ICT Project Management, Enterprise Architecture Design, Network and System Administration, Information System and Network Security, Mobile

[69] KOMINFO, http://bpptik.kominfo.go.id/profil-singkat/
[70] KOMINFO, http://bprtik.kominfo.go.id/index.jsp
[71] KOMINFO, http://bpptik.kominfo.go.id/uji-kompetensi-dan-sertifikasi/jadwal-pelatihan-dan-sertifikasi-bpptik-di-tahun-2015-2/
[72] KOMINFO, http://bprtik.kominfo.go.id/index.jsp

Computing, and Cloud Computing. Those skills will be recognised as the National Working Competency Standards (SKKNI)[73].

Formative: There is a perceived need to have more traditional and non-traditional training courses, as well as forums to discuss cybersecurity. There has been an identified need for more training of security professionals in Indonesia, particularly as the IT growth continues to expand in the country. ITB offers some training courses to the public and private sectors, but participants felt that other institutions that can provide licensed training courses should become more prolific. There was disagreement on whether more training should focus on the management of cybersecurity issues, or whether training should focus on operational skills. Both are needed in the country, but business leaders should collaborate to help prioritise the training needed. For example, IBM engages with other industries about incident management and malware detection. Additionally, in the telecommunications and financial sectors, some institutions have implemented programmes where new employees are given a session on corporate responsibility for cybersecurity. These programmes are ad-hoc at the moment and have not been proliferated outside of specific sectors. There is a need for MCIT to help develop incentive structures for training in these fields, since most of the training provisions are currently through international organisations or consultants. Encouraging domestic companies to provide cybersecurity training based on their experiences would not only help engrain incentives for a new training marketplace, but would also help tailor training provisions to the Indonesian context.

4.4 Corporate Governance, Knowledge, and Standards

This sub-dimension specifically looks into how private and state-owned companies, as represented by the highest executive level of senior management (C-level

[73] KOMINFO, http://kominfo.go.id/index.php/content/detail/6621/Siapkan+SDM+Kompeten+dengan+R-SKKNI+%3Ci%3ESoftware+Development%3C+i%3E/0/berita_satker#.Vt77i00fyUk

management), understand cyber security and react to changes related to the cybersecurity status quo. Any organisation represents a dynamic environment, where needs should be continuously assessed and addressed for the realization of an organization's mission and strategic goals.

Facts at a Glance: Corporate Governance, Knowledge and Standards

Boards and executives within ICT private and stated owned companies, such as PT Telkom and PT Indosat Ooredoo, have an understanding of how companies are at cyber risk in general. For example, in 2012, PT Telkom obtained ISO certification for their business processes within the business unit[74]. In 2015, PT Indosat Ooredoo received an ISO 27001 certification from the British Standards Institute for its information security management system[75].

Moreover, financial organization boards, such as the Indonesia Stock Exchange[76] and LPSE (National Procurement Agency), are also informed through the implementation of ISMS (Information Security Management System) [77].

Indonesia has six government organisations that are certified under internationally recognized standards in cybersecurity, such as ISO270001[78].

Start-up - Formative: Board-level understanding of cybersecurity issues is still evolving in Indonesia. Although boards and executives within state-owned enterprises and private sectors have some awareness of cybersecurity risks, this has been appraised as minimal. Even though, in most cases, board-level members are not usually trained in cybersecurity, organisations will need such cybersecurity certifications to support their business. The Indonesia Chamber of Commerce has been frequently approached about the relevance of cybersecurity to business operations, and needs help in navigating this issue. However, in terms of the boards receiving training on cybersecurity, they will either go abroad for such training, or will

[74] PT Telkom, http://www.telkom.co.id/assets/uploads/2013/05/SR-Telkom_2013_English_Final_lowres.pdf
[75] JakartaPost, http://www.thejakartapost.com/news/2015/12/10/indosat-offers-digital-service-corporate-customers.html
[76]IDX,http://www.idx.co.id/Home/NewsAnnouncement/PressRelease/ReadPressRelease/tabid/366/ItemID/efc1053e-31a0-47d1-92bf-365264cfdb1f/language/en-US/Default.aspx
[77] Kemenkeu,http://www.setjen.kemenkeu.go.id/Berita/awal-tahun-2013-pusat-lpse-raih-iso-270012005
[78] ITU, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Indonesia.pdf

remain ignorant of the general risks posed by cybersecurity. Some focus-group participants felt that the information security regulations in Indonesia should be forced onto state-owned enterprises, so that there will be some mandatory management of these issues. There is also a desire for MCIT to publish a guideline for information security structure at the corporate level, in order to help build board-level awareness. Finally, in the future, Indonesian ISPs hope to develop infrastructure portals to improve trust in e-commerce, assist standard implementation, and help provide certification for security. Such efforts would go a long way towards building the board-level understanding of cybersecurity risks.

4.5 Conclusion

In this dimension of cybersecurity capacity, Indonesia ranges between the *start-up* and *formative* stages for both education and training efforts.

- **National availability of cyber education and training**: Minimal educational offerings in cybersecurity exist. Some major universities, such as ITB and UI, offer a master's degree in electrical engineering in cyber security courses, but no accreditation in cyber security education exists. In terms of cybersecurity training, some local stakeholders, in cooperation with international training providers, provide training in information security. However, it is ad-hoc and uncoordinated with national education programs. A list of certified cyber security professionals is identified and considered as part of Indonesian National Work Competency Standards (SKKNI).
- **National development of cybersecurity education**: There are only a few professional instructors in cybersecurity. No formal programme exists to train instructors in cybersecurity, because the budget justification for education and research does not exist.
- **Training and educational initiatives within the public and private sectors:** Few trained IT personnel are designated to support cybersecurity training

programmes. Knowledge transfer from trained cyber security employees exists on an ad-hoc basis

- **Corporate Governance, Knowledge, and Standards:** Some boards have some awareness of cyber security issues, and some boards have an understanding of how companies are at risk in general.

5 Legal and regulatory frameworks

This dimension looks into the government's capacity to design and enact national legislation and accompanying by-laws, directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, cybercrime, and on the stakeholder groups represented by law enforcement, prosecution services, and courts. International experience attests to the crucial role that legal and regulatory frameworks play in mainstreaming cybersecurity across sectors, while presenting prevention, mitigation, and dispute mechanisms to individuals and organisations affected by cyber-threats.

5.1 Cybersecurity Legal Frameworks

This sub-dimension assesses the availability and comprehensiveness of ICT security and privacy and data protection legislation, its relation to human rights legislation, as well as the country's status in relation to regional and international treaties directly or indirectly related to cyber security.

Facts at a Glance: Cybersecurity Legal Frameworks

There is no standalone cybersecurity law in Indonesia. However, there are some Indonesian Laws subject to development in cybersecurity, as follows:

1. **Law Number 36/1999** on Telecommunications regulate any information in the form of sign, code, word, picture, sounds, and tone through cable system, fiber-optic system, radio, or other electromagnetic system[79]. This law does not regulate data protection or privacy through the Internet, but does cover network security issues.

[79] KOMINFO, Article 1 (1) of Law No. 36/1999, http://dittel.kominfo.go.id/wp-content/uploads/2013/06/36-TAHUN-1999.pdf

2. **Law No. 11 of 2008** on Electronic Information and Transactions (ITE) is the first cyber law in Indonesia and the main instrument for the regulation of online content and electronic transactions. The ITE Law contains provisions, such as (1) provisions on electronic information, records, and Signature; (2) provision of electronic certification and electronic systems, and electronic transactions; (3) domain names, intellectual property rights, and protection of privacy rights; (4) prohibited acts; and (6) investigation
3. **Law No. 14 of 2008** on Public Information Disclosure. This law regulates information that is produced, stored, managed, sent, and/or received by a Public Agency. The law states that every public agency is obligated to allow access to public information, except classified information. This law identifies the classification of classified information.
4. **Law No. 17 of 2011** on National Intelligence identifies the classification of government secrets
5. **Law No. 25 of 2009** on Public Service identified critical or strategic sectors for public services, such as education, health, energy, banking, transportation, natural resources, ICT, and tourism
6. **Law No. 23 of 2006** on Citizen Administration. This law contains provision of protection of Citizens' personal data, such as Date of Birth, Citizen Number, and family Certificate Number
7. **The Government Regulation No 82/2012** on the Electronic System and Transactions. It regulates 7 (seven) matters from the total 9 (nine) matters that need to be regulated by Government Regulations. These are Provision of Electronic Systems, Electronic Agent Operator, Provision of Electronic Transactions, Electronic Signature, Provision of Electronic Certification, Trust Mark Certification Body, and Domain Name Administration.

Formative: Partial legislation exists regarding ICT security, privacy, and data protection in substantive and procedural criminal law. The Electronic Information and Transaction (ITE) Law was the document most commonly referred to as the central document for punishing digital crime. However, many focus-group participants were confused as to what aspects of cybercrime/computer-related crime this law is meant to criminalise. According to some participants, the ITE includes components relating to cybercrime, illegal access, and computer related forgery. Much of this law was derived from the Budapest Convention, though Indonesia has not actually signed or ratified the convention. While some participants thought this law was sufficient to be classified as ICT Security regulation, other felt that this law is not sufficient to combat the various challenges facing the legal system. Some claimed that Internet Service Providers (ISPs) need additional legislation to criminalise the illicit use of their

networks and mandate cooperation between ISPs and police. Some participants felt that a cybercrime-specific law is still required to fully address the problem. The MCIT has proposed a draft law, titled Draft Information Technology Crime Act ("UU TIPITI"), which would seek to supplement the ITE, but this has not been passed. Some focus-group participants proposed that MCIT pushes the ministerial degree to pass a more cyber-specific legislation, due to the extended time necessary to pass more formal legislation. As previously mentioned, there is no comprehensive legislation on data protection or privacy in Indonesia. Some participants indicated that the government is developing a law on personal data, but the expected timeframe for this law is far in the future. According to Article 15, paragraph *c,* of Regulation No. 82/2012, “the data collector must guarantee that the use or disclosure of personal data is implemented based on prior consent from the data subject. The data collector must also make sure that the data is used in the way it was stated it would be in the initial notification given about the purpose of the data collection.” While this is a step toward ensuring more substantial data protection, there is no data protection commissioner in Indonesia, nor is any other regulatory body responsible for ensuring this law is abided by. Further elaboration on the roles of data collectors (both public and private) would help make data protection and privacy more transparent. The ITE law, while addressing some cybercrime issues, has encountered several implementation challenges. According to the focus-group participants, synergising regulations across the various levels of legislation is difficult. For example, there are often cases when ministries and local government have their own unique regulation, therefore complicating coordination. Due to the geographically disparate regions in Indonesia, there is often a bias about the interpretation of the legislation as it applies to the local context. The ITE law has gone through a synchronisation process, but participants claim that this has not reached the local level. Procedural law for investigating cybercrime is contained within the ITE law, but procedures for the preservation of evidence are not included in this document.

5.2 Legal Investigation

This sub-dimension studies the capacity of the executive branch of the government to prevent, combat, and investigate cyber incidents, attacks, and crimes, and of the judiciary branch to prosecute cybercrime and electronic evidence cases. It also looks into the dynamic of formal and informal collaboration between different branches of government, and between the government and court system.

Facts at a Glance: Legal Investigation

The capacity of law enforcement authorities to prevent and combat computer-related crimes exists in Indonesia, as follows:

1. According to the Law No.11/2008 in Article 43, the State Police of the Republic of Indonesia and Civil Service Officials with the Government, whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions, shall be granted special authority to investigate computer-related crimes or cybercrime.
2. The State Police of the Republic of Indonesia (POLRI) has a cybercrime unit, which is responsible for conducting investigations of criminal acts of Information Technology, Telecommunications, Electronic Transactions, and Intellectual Property[80]
3. The Division of Forensic and Law Enforcement under the Directorate of Information Security has a technical capacity to carry out an investigation, law enforcement, searches, and/or seizures in relation to criminal acts of Information Technology and Electronic Transactions[81].
4. Institutional capacity to prosecute and handle cybercrime cases and cases involving electronic evidence is established, in which POLRI has a Digital Forensic Laboratory - Cyber Crime Investigation Centre (CCIC) that is accredited by National Standardization Agency of Indonesia[82].

Formative: Law enforcement capacity is varied in Indonesia. Some investigative capacity exists to investigate a computer-related crime. At the national level, there is a cybercrime unit within the police, designated to investigate cybercrime. There is

[80] POLRI, http://www.reskrimsus.metro.polri.go.id/struktur-organisasi/kasubditIV
[81] KOMINFO, http://www.aptika.kominfo.go.id/index.php/profile/direktorat-keamanan-informasi
[82] BSN, http://sisni.bsn.go.id/index.php?/lembinsp/inspeksi/detail/8710

also an investigative capacity of civil investigators, although the police will normally provide the training for such units. There is some digital forensic capacity, but since there is only one lab within POLRI, the focus must be on major incidents, which limits the scope of the investigation. There was some confusion among participants regarding the differences between the role of the civil investigators and the police when investigating cybercrime cases. Clarifying the roles and responsibilities of different investigative capacities would enable more effective communication of cybersecurity issues with the authorities.

Overall, there is a lack of capacity in prosecution services and the judiciary to effectively prosecute a cybercrime case, or even a case utilising digital evidence. Both parties often prefer using physical evidence when possible, and even when there is only digital evidence, there is often confusion as to how to process such evidence. While few cybercrime cases go to court at the moment, additional training to both the judiciary and prosecution would enable better processing and evaluation of digital evidence in the legal system.

5.3 Responsible Reporting

This sub-dimension explores if the public and private sectors enact a responsible disclosure policy, and if there is sufficient capacity on the part of both to continuously review and update this policy and synchronise it with recognised international and responsible disclosure mechanisms. It also analyses the existing capacity of stakeholders to receive, analyse, and disseminate vulnerability information, gleaned through the responsible disclosure mechanisms

Facts at a Glance: Responsible Reporting

Such a vulnerability disclosure provision is in place in Indonesia, but it is limited. Article 15 of the Government Regulation No.82/2012 in Section 2 requires that, in a case of failure in protecting the secrecy of personal data that it manages, Electronic System Operators shall give written notification to the owner of the personal data.

Start-up - Formative: The need for a responsible disclosure policy in public and private sector organisations is not acknowledged, even though a vulnerability disclosure provision is in place in Indonesia. According to most of the focus-group participants, there is no formal responsible disclosure mechanism for organisations and companies to report cybersecurity incidents. Banks often do not report incidents, due to their concern about repercussions to their reputation. Representatives from MCIT asserted that ITE law provides a framework for responsible disclosure, but none of the other participants were aware that such a mechanism exists. However, later on, the participant from MCIT said it is not a disclosure framework, even if it is briefly stated in the government regulation No 82/2012. Promoting the existence of such a mechanism, or else refining the requirements of that framework to include specific instructions regarding disclosure timeline, would help enhance maturity in this capacity.

5.4 Conclusion.

The stage of maturity for legal and regulatory frameworks in Indonesia varies, depending on the legislation in question.

- **Cybersecurity legal frameworks**: Legislation and legal frameworks relating to ICT Security have been implemented. Legislation protecting the rights of individuals and organisations in the digital environment has been adopted. Privacy and data protection legislation does not exist, but partial legislation exists regarding privacy, data protection, and freedom of expression, such as Law No. 11/2008 and the Government Regulation No. 82/2012. In terms of substantive cybercrime law, Indonesia has adopted international instruments on cybercrime into the national law No. 11/2008. This law covers substantive criminal law for cybercrime. For procedural cybercrime law, a comprehensive criminal law with procedural powers for investigation of cybercrime, and evidentiary requirements to investigate, law enforcement, and prosecute

cybercrime, has been implemented. In the case of a cross-border investigation, the law no 11/2008 covers this matter.

- **Legal Investigation**: The capacity of law enforcement authorities to prevent and combat computer-related crimes exists. Some capacities to investigate and manage cybercrime cases have been established, such as digital forensic laboratories in POLRI and KOMINFO. These capacities are meant to investigate computer-related crime, in accordance with the ITE law No. 11/2008. Resources are dedicated to the operational cybercrime unit in POLRI and the division of investigation and law enforcement in KOMINFO. A limited number of prosecutors have the capacity to build a case based on digital information, even though the institutional capacity to prosecute and handle cybercrime cases is established. Insufficient human training and technological resources still exist. A limited formal mechanism of international cooperation to prevent and combat cybercrime is in place. There are no separate court structure or specialized judges for cybercrime cases and electronic evidence. A very limited number of judges have the capacity to preside over a case on cybercrime, and judicial resources or training in cybercrime is very limited.
- **Responsible Disclosure:** Such a vulnerability disclosure provision is in place, in accordance with the government regulation No. 82/2012, but it is limited and only related to the secret of personal data. In the case of information disclosure related to personal data, public and private sectors entities are required to report any information related to hacking or cyber-attacks, in which personal data is compromised.

6 Standards, organisations, and technologies

This dimension introduces the importance of implementation of cybersecurity standards and, at least, minimal acceptable practices, the existence of well-functioning and high-capacity organisations coordinating cybersecurity with formal authority over multiple stakeholders, and the existence of a vibrant cybersecurity marketplace of technologies and cyber-insurance services.

6.1 Adherence to Standards

This sub-dimension assesses the government's capacity to design or adapt from other jurisdictions, and implement, cybersecurity standards and minimal acceptable practices, especially those related to procurement procedures and software development. These standards and practices provide a minimally necessary baseline, in the context of which strategic government decisions, especially organizational (resource) and financial (budgetary) ones, should take place.

Facts at a Glance: Adherence to Standard
The past three years have seen a number of new cybersecurity standard adoptions in Indonesia; what follows is a selection:

- **SNI ISO/IEC 27001:2013:** Indonesia has adopted SNI ISO/IEC 27001:2013 on Information Technology – Security techniques – Information security management systems – Requirements. This National Standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization[83].
- **SNI ISO/IEC 15408-1/2/3:2014:** Indonesia has adopted a common criteria, also known as ISO/IEC 15408 on Information Technology — Security techniques — Evaluation criteria for IT security, Part 1 (ISO/IEC 15408–

[83] BSN, http://sisni.bsn.go.id/index.php?/sni_main/sni/detail_sni_eng/16218

1:2009, IDT)[84], Part 2 (ISO/IEC 15408-2:2008, IDT)[85], and Part 3 (ISO/IEC 15408-3:2008, IDT)[86]. This standard is meant to be used for evaluation of security properties of IT products, including software.

- **SNI ISO/IEC 15504-5:2015:** Indonesia has adopted SNI ISO/IEC 15504-5:2015 on Information Technology – Process Assessment. This standard is a set of technical standards documents for the computer software development process and related business management functions.

It has to be noted that BSN (National Standardization Agency) is mainly concerned with the adoption of the ISO/ IEC-based standards, as well as its home-grown standards. However, many other standards, such as those set up by ITU or by IETF, are not yet considered for inclusion in the program to adopt international standards into Indonesian national standards (SNI).

Formative: Information security standards have been identified for use, but there is a minimal implementation of national and international standards. Several national level institutions have adopted the ISO 27000 series security standards, including the data centre, financial sector, health sector, and individual ministries, but the degree to which all of the standards are implemented has not yet been determined. The ITE law stipulates which ministries/sectors should adopt the standards, but there is no monitoring of standards implementation at this point. According to focus-group participants, the industry more frequently adopts internal standards for business requirements, but there is no mandatory requirement that any industry do so. Even regulators, for example, in the telecommunications sector, do not necessarily strictly assess compliance. For procurement security standards, LKPP bases its procedures on ISO standards, and the national cryptography agency works with LKPP to ensure that product development meets security standards. However, while e-procurement systems have proposed security measures through LKPP, there is no organisation that mandates implementation, nor is there a body responsible for monitoring such implementation. For software development, each product must undergo vulnerability testing to determine holes in the software. However, actual software development security standards are subjected to the same ad-hoc implementation as ICT security

[84] BSN, http://sisni.bsn.go.id/index.php?/sni_main/sni/detail_sni_eng/20374
[85] BSN, http://sisni.bsn.go.id/index.php?/sni_main/sni/detail_sni_eng/20375
[86] BSN, http://sisni.bsn.go.id/index.php?/sni_main/sni/detail_sni_eng/20376

standards and procurement security standards. Regular review of security standard implementation across sectors, as well as the designation of a ministry responsible for monitoring implementation, would help increase maturity in this capacity.

6.2 National Infrastructure Resilience

This sub-dimension assesses how effectively the government deploys and manages infrastructure technologies (the government's own networks and systems), and how it performs monitoring and evaluation of the costs for infrastructure technologies and their resilience. Also, it looks into the existence and exercise of the government's capacity to engage in strategic planning and maintain sufficient scientific, technical, industrial, and human capabilities.

Facts at a Glance: National Infrastructure Resilience

The following information is re-written from an academic paper, entitled, Towards data sovereignty in cyberspace[87].

According to the Indonesian Internet Service Provider Association (APJII), the number of Internet users will grow from 88.1 million in 2014 to 139 million by 2015[88]. PT Telkom is Indonesia's largest telecommunications company, with 9.52 million fixed-wire-line customers, 28.69 million fixed-wireless customers, and 137.37 million cellular customers, as of June 2014[89]. PT Indosat is Indonesia's third-largest cellular operator, with more than 59.7 million cellular subscribers[90]. The government of Indonesia retains shares in both companies, including over 50 percent ownership in the case of PT Telkom.

Indonesia has more than 300 Internet Service Providers (ISPs) and Network Access Points[91], which include big operators such as PT Telkom and PT Indosat, who own their network infrastructures. The fibre-optic Palapa Ring network is currently being implemented throughout Indonesia, in order to accommodate such

87 Nugraha, Y.; Kautsarina; Sastrosubroto, A.S., "Towards data sovereignty in cyberspace," in Information and Communication Technology (ICoICT), 2015 3rd International Conference on , vol., no., pp.465-471, 27-29 May 2015
doi: 10.1109/ICoICT.2015.7231469

88 APJII, http://www.apjii.or.id/v2/read/content/info-terkini/301/pengguna-internet-indonesia-tahun-2014-sebanyak-88.html

89 PT Telkom, http://www.telkom.co.id/kinerja-telkom-semester-i2014-tumbuh-meyakinkan.html

90 Telegeography, https://www.telegeography.com/products/commsupdate/articles/2014/05/09/indosat-surges-back-into-profit-after-years-of-losses/

91 Citizenlab,https://citizenlab.org/wp-content/uploads/20131101IIX-APJII2012-APNIC34-Final.pptx

a national broadband plan. The Palapa Ring project contains 35,280 kilometres of undersea cable[92]. Many of these submarine cables connect to Singapore, which serves as a major hub for submarine cables used for Internet and telecommunications infrastructures between Asia Pacific and Europe.

Regarding international connections, Indonesia is currently linked to only one intercontinental cable, the South-East Asia-Middle East-Western Europe 3, called the SEA-ME-WE3, which is the longest optical submarine cable in the world, with landing points in Medan and Jakarta. This optical fibre submarine cable runs 39,000 kilometres from Europe, through the Middle East, across to South-east Asia and Korea via China and Japan. Indonesia has no direct connection to the Asia-America Gateway, a 20,000-km cable running from the US West Coast across the Pacific Ocean to South-East Asia[93]. However, recently, the new SEA-US submarine cable system is being developed through the five areas and territories of Manado (Indonesia), Davao (Philippines), Piti (Guam), Oahu (Hawaii, United States), and Los Angeles (California, United States). The submarine cable will run approximately 15,000 kilometres in length[94].

Formative: Online government services, information, and digital content are available online, but implementation and process are limited. National infrastructure is managed informally. Infrastructure resilience at this national level is currently subjected to annual surface level agreements within each provider's contract, which includes security requirements. Several private sector organisations felt that it would benefit from non-annual contract agreements, so that a more regular security implementation can be maintained. Furthermore, it was discussed in the focus groups that access and availability of network infrastructure is still lacking at the local level, and reliability of existing infrastructure provision is still questionable. PT Telkom and PT Indosat are the two providers for infrastructure resilience, but additional industry collaboration is required to ensure more support for this resilience effort. There is also reliance on Singapore for international connectivity, and, although cooperation between the countries is positive, Indonesia is seeking to work on an undersea backbone for an eastern port to improve resilience efforts. There is still a need for better and more secure connectivity in the western part of the country.

92 Oxford Business Group http://www.oxfordbusinessgroup.com/news/indonesia-building-capacity-data

93 Oxford Business Group, ttp://www.oxfordbusinessgroup.com/analysis/network-news-improving-international-connectivity-among-items-agenda

94 NEC, http://uk.nec.com/en_GB/press/201408/20140828_01.html

6.3 Cybersecurity Marketplace

This sub-dimension studies the availability of competitive cybersecurity technologies and their strategic deployment and maintenance by public and private sectors. It also assesses the state cyber insurance marketplace and its offerings, through the study of the perception of financial risks by the public and private sectors, and perceived demand for cybercrime insurance.

Facts at a Glance: Cybersecurity Marketplace

According to The Masterplan for Acceleration and Expansion of Indonesia's Economic Development (abbreviated MP3EI), In Indonesia[95], the ICT industry structure can be described in the form of layers, as follows:

- Layer 0: Content Industry
- Layer 1: ICT Application Industry (e-Government, e-Health)
- Layer 2: Access Services Industry
- Layer 3: Infrastructure Services Industry (network provider)
- Layer 4: Integration, Installation, and Maintenance System Industry of ICT Device
- Layer 5: ICT Device Manufacturing Industry
- Layer 6: ICT Device Component Industry
- Layer 7: CT Device Component Material Industry

Most ICT components are mainly dominated by foreign products (60%), and only 30% of joint assembly is conducted for software design in-house.

Start-up: There are no cybersecurity technologies produced domestically. Though the marketplace for cybersecurity products in Indonesia currently uses indigenous cryptographic programmes for ministry efforts (which are mandatory for government programmes), they do not produce technology products. Moreover, the private sector still relies heavily on imports from various international sources and, since there is no certification authority, reliance on imports is likely to persist. The insurance market in Indonesia is primarily dominated by foreign firms, but participants felt that a lack of understanding of cybersecurity undercuts the demand for such coverage.

[95] Kemlu, http://www.kemlu.go.id/rome/Documents/MP3EI_PDF.pdf, page 86

6.4 Conclusion

In terms of cybersecurity standards adoption and implementation, there is ad-hoc adoption at the national level, with even less applied at the local level.

- **Adherence to standards:** Information security standards have been identified for use, such as ISO/IEC 27001. There have been some initial signs of promotion and take-up within government agencies, public sectors, and CNI organisations. In a case of the adoption of SNI ISO/IEC 27001, there is a minimal implementation of national and international standards. In most cases, SNI ISO/IEC 27001 is widely used for guiding government procurement processes for security requirements, even though Indonesia has adopted SNI ISO/IEC 15408 on Information Technology — Security techniques - Evaluation criteria for IT security. Methodologies for software development processes have been discussed and promoted by government and professional communities through SNI ISO/IEC 15504-5:2015.
- **National Infrastructure Resilience:** Technology and processes deployed meet international IT standards, guidelines, and best practices, such as COBIT. In some cases, the Internet is widely used for e-commerce and electronic transactions. However, rigorous security processes are under development, especially for security risk management, threat assessment, incident response, and business continuity. Regular assessment of processes and national information infrastructure security according to standards and guidelines are still being discussed. State-owned companies, such as PT Telkom, manage national communication infrastructure. The government has minimal control of its own infrastructure, network, and system, which are outsourced. In most cases, there is a dependence on other countries for cyber security technologies.
- **Cyber security marketplace:** No cyber security technologies are produced domestically. In most cases, foreign providers produce security technologies and solutions, and those are widely used in government agencies and private sectors. The need for a market in cybercrime insurance has not been considered as an important aspect for the public and private sector.

7 The Future of Cybersecurity Capacity

Effective cybersecurity capacity includes early warning, prevention, detection, resistance, and recovery capabilities. The Government of Indonesia needs to effectively identify its national assets, organisations, allies, and adversaries to seize the full benefits of emerging trends in the Internet, and to be able to operate from a defensive posture.

Today, governments, businesses, and civil society are encouraged to conduct transactions and participate online, and the risks will increase accordingly. Hence, it is important to develop cybersecurity capacities, such as awareness, education, and training in cybersecurity, ranging from pupils, undergraduates, postgraduates, apprentices, employees, IT specialist, board, and senior government officials. This initiative should first increase the cybersecurity awareness for all key national multi-stakeholders in Indonesia, and then, later, it should encourage them to develop their capabilities relating to Internet governance and cyberspace. This will certainly be followed by other developments needed to strengthen cybersecurity capacity. This cybersecurity awareness initiative can perhaps best be shown by the fact that most people do not understand the need to secure cyberspace components, and neither do they know how to classify such capabilities according to threats. For example, in Indonesia, the telecommunication cables and Internet, connected to government agencies, industries, homes, etc., are mainly installed outside, unmarked, and erected using unidentified ducts and poles. Hence, there is a need for government intervention through effective legal and regulatory frameworks, because the government agencies, industries, and individuals need to be confident whether their data are effectively protected and secure, in order to gain the many benefits of a digital environment. As the country begins to seize the full benefits of ICTs, effective regulation, coordination, and awareness campaigns, along with the use of

cybersecurity solutions, are necessary to protect national data and infrastructure, as well as to strengthen cybersecurity capacity in Indonesia.

7.1 Opportunities and Threats

Indonesia is one of the largest social media users in the world. For example, Indonesia has become the main market for social media platforms, such as Facebook, Twitter, and WhatsApp, and is clearly the biggest and most enthusiastic user of social networking in the region[96]. As such, Indonesia presents a potential opportunity for anyone providing cybersecurity solutions, especially for public services. Indonesia is currently one of the most countries in the region that is open to solutions from foreign investors, such as the creative industry, e-commerce, and healthcare services[97], except for defence industries.

No government will be able to handle the cyber threat alone. Cyber threats posed by any adversary, such as cybercrime, will increase, which necessitates increasing public and private organisations' investment over the next 5-10 years. This increase in investment could provide opportunities for cybersecurity service provision to public services and CNIs, including government sector organisations. The Government is currently relying on third party companies both from local and foreign suppliers. For example, various cybersecurity solutions, in particular for public services and financial institutions, are widely implemented. However, as cybersecurity risks increase, domestic markets can embrace this change as an opportunity for market development.

Such foreign direct investment through ASEAN Economic Community could boost the ICT Sectors in Indonesia. Indonesia should attract more foreign companies to

[96] Techniasia, https://www.techinasia.com/indonesia-web-mobile-data-start-2015
[97] Channelnewsasia, http://www.channelnewsasia.com/news/business/international/indonesia-opens-up-20/2507182.htm

invest in Indonesia. For example, Indonesia has strong ties with Korea, Japan, and China suppliers. Indonesia could leverage its strong position in ASEAN to encourage cyber-related investment from those countries. Raising cyber standards is essential for business security, such as small and medium-sized enterprises (SMEs). As part of the e-commerce roadmap, the Government wanted to produce up to 1,000 SMEs and IT Startups by 2020[98]. Successful ICT adoption and socialisation resulted in increased ICT applications by SMEs, which, unfortunately, still underestimates the need for cybersecurity. With intensive developments on ICT applications by SMEs, it will not be too long before they have to improve their cybersecurity capacity. As SMEs often neglect it, cybersecurity for SMEs is necessary as an integral part of Indonesia's economy, in order to boost e-commerce at a national level. However, there is a very low level of knowledge of cybersecurity amongst consumers and providers. Nevertheless, the SME sector as consumers could serve as potential contributors to the development of cybersecurity markets in Indonesia. If Indonesian SMEs increase cyber security awareness of the potential cyber threats facing their business, this can drive levels of cyber investment that we have not seen to date. The increasing dependence of SMEs on digital environments is the biggest driver behind this trend.

The biggest opportunity for the Indonesian cybersecurity sector may well lay in the provision of operational expenditure (OPEX), rather that capital expenditure (CAPEX). Such government and private organisations tend to buy services, rather than products, from suppliers and third party companies. However, as stipulated in the Government Regulation 82/2012, there are some measures about the use of foreign OPEX and CAPEX, among which are that the data centres have to be located in Indonesia, the experts should be Indonesians, and the source code of the software used has to be surrendered to the Government. Nevertheless, the public

[98] Tempo, http://en.tempo.co/read/news/2016/02/18/056746079/Jokowi-Targets-to-Produce-1000-Technopreneurs

service and private sectors need guidance in cybersecurity best practice; what works and what does not work, what is needed for investment, and what is not necessary.

There is a possibility to increase the number of Indonesian security experts in ASEAN markets. Singapore and Malaysia are already pursuing an agenda to promote the National Cyber Security in their countries, which are purchasers of other security offerings, such as human resource, from Indonesia.
In terms of threats, the biggest challenges are that Indonesia still relies on foreign companies for Internet technologies and cybersecurity solutions, such as Facebook, Google, Microsoft, Symantec, and VeriSign, which are almost all U.S.-based companies. Also, Indonesia's national communications networks are currently managed by China's two leading telecommunications suppliers, Huawei and ZTE. Those companies could pose a national security threat to Indonesia, as well as threaten local industries. Also, Korea and Japan are currently very open to funding cybersecurity capacity building in Indonesia, through cybersecurity programs run by Korea International Cooperation Agency (KOICA) and Japan International Cooperation Agency (JICA). It could make Indonesia rely on those two countries in terms of the development of cybersecurity capacity in Indonesia. Moreover, although foreign companies are likely to acquire and join local industries, a lack of cybersecurity skills could drive dependence on foreign capability. It demonstrates the relative lack of local expertise in cybersecurity.

A lack of accreditation and cybersecurity standards exists. This is particularity an issue where international standards exist, but are duplicated by, or rejected in favour of, sub-adequate local standards. Suppliers are forced to choose between access to domestic customers and international markets. It leads to cases where national industries work with foreign companies, but not those in their own country. For example, the convergence between SNI ISO/IEC 27001 and the internationally recognized ISO/IEC 27001, is seen by many suppliers as a major imperative for e-procurements, but it is moving slowly. Moreover, there is an increasing expectation

that services be procured over the Internet, but security controls against specific threats do not exist. Also, it is worth noting that the National Standardization Body of Indonesia (BSN) mainly uses the ISO/IEC as the source of Indonesian standards. Other telecommunications and Internet standards, such as ITU-T from ITU or RFCs from IETF, are rarely recognised. This is also true for other security standards and best practices, such as ANSI/TIA 942 for data centre security tier level standard and NIST.

It has to be noted too that Indonesia's trend is to open to more international cooperation and legal framework, which may rapidly increase cyberspace economics, such as e-commerce. For example, Indonesia ratified the WTO's Information Technology Agreement (ITA)[99], which will certainly help to increase ICT equipment import-export businesses in Indonesia. Indonesia also agreed to the WTO arrangement that makes no barriers to any transfer of software in cyberspace. On the other hand, the weak development in cybersecurity will pose a threat to this development, but international business cooperation will certainly support cybersecurity development in Indonesia. Otherwise, the business cooperation will pose a bigger threat.

[99] WTO, https://www.wto.org/english/news_e/brief_ita_e.htm

7.2 Strengths and Weaknesses

Indonesia's population is the fourth largest worldwide and one of the world's largest economies. Concerning its economy, education accounts for a high proportion of the national budget, and now has the full authority to manage a big portion of Indonesia's education budget through the Indonesia Endowment Fund for Education (LPDP). In the education sector, Indonesian universities, such as Bandung Institute of Technology (ITB) and University of Indonesia (UI), have some cybersecurity courses and are fostering close ties to government organisations. In terms of international cooperation, Indonesia engages in several, mainly regional, multilateral technical and policing forums, including AP-CERT, FIRST, ASEAN-Japan Information Security Forum, ASEAN Network Security Council (ANSAC) Working Group, ITU-IMPACT, Internet Governance Forum, and ICANN. The plan to launch Indonesia's National Cyber Agency should help to manage its International engagement in relation to national interests.

However, Indonesia lacks a cybersecurity education strategy. There is no dedicated budget for a cybersecurity programme, in particular. Indonesia also lacks any joint Public-Private Partnership (P2P) to address cybersecurity, as there is no dedicated public-private sector plan in Indonesia. Moreover, there is a lack of accreditation for suppliers in government procurement. Consumers use retail outlets and small resellers to purchase IT equipment. There is no widespread certification and accreditation that give confidence to customers, except telecommunication equipment, such as mobile phones, because those have national certifications from MCIT. Also, a lack of customers' knowledge exists because many government agencies, for instance, from senior levels down, lack knowledge of most established cybersecurity technologies and practices. Their understanding of cybersecurity threats and their impact is very limited. They normally do not understand why they should invest in cybersecurity measures, such ass anti-virus products.

7.3 Recommendations for Indonesia Government

Recommendation #1: Develop a national cybersecurity strategy (NCSS)

As stated, Indonesia has delivered on its plan of a National Cyber Agency. Currently, the National Desk on Resilience and Cyber Security (DK2ICN), under the Coordinating Ministry for Political, Legal, and Security Affairs (POLHUKAM), is in charge of establishing a National Cyber Agency in Indonesia through a draft of a Decree of the President of Indonesia. In the meantime, the Directorate of Information Security, under the Ministry of Communications and Information Technology (KOMINFO), is currently working on the development of a Cyber Security Master Plan.

It is recommended that POLHUKAM and KOMINFO, as leading agencies in this process, as well as other government ministries with a mandate in ICT sector development, should be involved in the effort of developing a national cybersecurity strategy. It is important that the development of the strategy should be premised on multi-stakeholder consultation with national entities. A strong consensus for developing a national cybersecurity strategy is of paramount importance to boost cybersecurity capacity and raise awareness of cyber culture.

Moreover, the plan to create a cybersecurity strategy should be in line with the development of a Government strategy to develop the Government ICT Infrastructure, as stipulated in Presidential Decree 96/2014 on National Broadband Plan. If a national government CIO is appointed, then a unit for cybersecurity would also have to be set up. The strategy should clearly distinguish between the role of KOMINFO as the ICT Infrastructure regulator, and other ministries/institutions as sectoral regulators, including the use of ICT applications in the sector. Cybersecurity should be embedded in their role as the regulators, hence, showing the importance

of awareness as well as capabilities in cybersecurity for all regulators. Also, it should be noted that the strategy should include developments of other related Internet Resources, directly or indirectly related to cybersecurity, such as the Certification Authority (CA), Internet Protocol (IP), and Autonomous System (AS) Numbers, as well as Domain Name System (DNS) in Indonesia. In this case, the strategy to develop the national Internet infrastructure has to be included, such as the set-up of an international gateway for Indonesia, and the national filtering system.

DK2ICN, along with Directorate of Information Security, should be responsible for drafting a national cybersecurity strategy, with consultation from other stakeholders in society. International consultation may also assist with the development of such a strategy. The content of such a strategy should be based on national risk priorities. The lead agency should coordinate with other government ministries, critical national infrastructures, private sector entities, and civil society to ensure the strategy is appropriate for all of Indonesia.

In case of Indonesia, a national cybersecurity strategy can be stated in the form of regulation, such as a Decree of the President of Indonesia. A notable improvement in an organisational structure, such as a Cyber Security Agency of Indonesia, can be formed after the Presidential Decree has been signed and issued. The aim of the agency would serve as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts at a national and international level.

Therefore, it may be optimal for Indonesia to start working on the development of the national cybersecurity strategy before the establishment of a National Cyber Security Agency (NCSA) of Indonesia. The Presidential decree should regulate coordination between government stakeholders and law enforcement, as well as other related entities, to address the implementation of cybersecurity capacity in Indonesia.

Recommendation #2: Strengthen the role and coordination function of ID-SIRTII/CC as a national CERT.

KOMINFO needs to further improve its role and coordination function as a leading agency for cybersecurity incident response. As stated, both ID-SIRTII/CC and GovCSIRT are managed and funded by KOMINFO's budget. However, the operations of those agencies are conducted separately under different Directorate General as First Echelon Level of KOMINFO. Worth mentioned is that this National CERT should be able to cover the Communities' CERT as well as the local Government CSIRT. Improving the current and future sector CSIRTs is important to improving capacity. This should also include a centralized registry of cybersecurity incidents.

Therefore, it may be optimal for Indonesia to set up a single entity to regulate and control cybersecurity, such as assigning the Directorate of Information Security as a government entity responsible for the establishment of a National CERT in Indonesia. The existing ID-SIRTII is currently considered as a Coordinating Centre, but it is not widely recognised. Moreover, the operations of ID-SIRTII should be under the control of the Directorate of Information Security that can manage ID-SIRTTI/CC instead of the Directorate of Telecommunications. However, there are some financial and administrative constraints that need to be discussed and solved within KOMINFO.

Recommendation #3: Create a formal list of CNIs on multi-stakeholder consultation, and work with the companies that own and manage CNIs.

A list of CNIs agreed upon by the government should be formally publicised. As stated, in 2013, the Indonesian National ICT Council (*Dewan TIK Nasional - WanTIKNas*) created a list of CNIs and identified 11 critical national infrastructures, but it is not considered as a formal list of CNIs. Also, the Ministry of Defence

established a list of CNIs in 2013 and identified 12 critical sectors through their Roadmap for National Cyber Defence Strategy, but is not widely recognised and not determined on multi-stakeholder consultation.

Reporting requirements between CNIs and their relevant government ministries should also be agreed upon, including determining the scope of cooperation between CNIs and the lead government agency. Full implementation of response planning and risk management should be agreed upon, incorporated, and monitored for these organisations. Additionally, it is worth noting that the Indonesian National Police (POLRI) operates a directorate for the protection of national vital objects (*PamObVit*) that is especially tasked with securing national vital objects, which are officially recognised as vital objects by the Indonesian Police. The object then receives special police guards. This method can be extended to cover CNIs, but it has to be made clear by the Government which institution has the authority to protect CNIs in Indonesia that are categorised according to its criticality and the national impact of its loss. For example, the UK Government established the Centre for the Protection of National Infrastructure (CPNI) to provide protective security advice across the UK's critical national infrastructure, as well as help ensure the UK's security and resilience.

Therefore, it may be optimal for Indonesia to establish a priority listing of CNI assets in the threat environment. In particular, the list highlights the crucial role of closer cooperation and coordination between the owners and operators of CNI assets, and national security ministries and agencies. It will delineate how the Government will protect national security and support economic prosperity through the establishment of trust between the government and CNIs with respect to cybersecurity and exchange of threat information.

Recommendation #4: Conduct crisis management exercises at a national level by inviting the relevant key national stakeholders to ensure preparations for national cyber incident responses are well managed and robust.

It is recommended that a leading agency, responsible for cybersecurity incident in Indonesia, should conduct exercises-simulations at the local and national levels at least once a year. Crisis management exercises should also include non-technical capacities, such as a cyber-policy hackathon and decision-making process exercises during the crisis. As stated, ID-SIRTII annually conducts a National Drill as a crisis management in the form of competition.

Therefore, it may be optimal for the Government to conduct technical and non-technical simulations at a national level dealing with national cyber incidents. The simulations would be expected to provide valuable insight, and inform the overall crisis management for all stakeholders and a better decision-making process. Moreover, the exercise should address national and international challenges, and produce scalable results for policy development strategic decision making. It is worth including outside observers to participate and contribute to the process.

Recommendation #5: Create and build dedicated civilian and military capability to help ensure that Indonesia has the capability to protect national interests in cyberspace.

The Ministry of Defence, if it chooses to have a role in managing national cyber defence, should enhance coordination within other responsible ministries so that clear roles and responsibilities are established. Developing a cyber-defence strategy might make these coordination and organisation mechanisms more transparent. Also, it is necessary to include the military's position concerning national infrastructure resilience in its response to different types and levels of cyber-attacks.

Therefore, it may be optimal for Indonesia to create a national cyber defence policy and strategy This strategy should include cyber defence capability requirements that are agreed upon between the public and private sectors, in order to minimise threats to national security. This strategy can be implemented through a cyber-defence unit

that is incorporated into the different branches of the armed forces, along with a civilian cyber reserve corps.

Recommendation #6: Establish emergency response asset priorities in the event a service failure occurs that are aimed at reducing impact.

As stated in the Government Regulation No. 82/2012, Electronic System Operators for Public Services must have a business plan and a recovery centre. Mapping critical assets and redundancy efforts for proliferation among stakeholders in the government and externally would raise the maturity of redundancy efforts. As stated in Presidential Decree number 96/2014, a data recovery centre is a must, and all these data centres, as well as the disaster recovery centre (DRC), should be integrated to form the Government National ICT Infrastructure.

Therefore, it may be optimal for Indonesia to establish emergency response asset priorities and standard operating procedures in the event of a computing, communications, and storage services disruption.

Recommendation #7: Develop a cybersecurity communication strategy to strengthen and expand the national cybersecurity campaign.

The newly designated organisation responsible for cybersecurity capacity should ensure that, in its remit, it is also responsible for enhancing the socialisation of cybersecurity across all sectors of society. This socialisation should include the establishment of a national awareness campaign that seeks to raise awareness of cybersecurity among citizens. If a national campaign is not possible at this point, targeted campaigns should focus on particular groups, such as ministries, business leaders, children, or other demographics. Currently, there are several government organisations doing cybersecurity socialisation. To make sure that all efforts are carried out based on a similar platform, a close coordination is certainly needed. It is

worth noting that socialisation on cybersecurity should be started by increasing security mindset and awareness.

Therefore, it may be optimal for the government to promote greater levels of cybersecurity mindset across government agencies, businesses, and civil society at all levels. It is also necessary to promote greater levels of cybersecurity best practices through programmes and materials that are available publicly, so that society at large can access the information.

Recommendation #8: Develop a single authoritative online portal for cyber raising awareness amongst governments, businesses, and civil society across the country.

As stated, the number of Internet users online is increasing rapidly. Hence, there should be a single online portal for cyber raising awareness that is curated by a responsible party. This service should be able to be accessed by any means of communications and devices. Currently, as mentioned in point 7, cybersecurity awareness is socialised by several government institutions. Each government institution usually has its own portal and program. As a start, at least, all portals related to cyber raising awareness should be linked to one another.

Therefore, it may be optimal for the government to establish national awareness-raising campaigns closely linked to a national cyber security strategy with defined targets, covering all multi-stakeholders in Indonesia. It will be effective to develop a single online portal through multi-stakeholder engagement for delivery of awareness raising IT products and services.

Recommendation #9: Promote greater levels of trust in online services, such as e-government and e-commerce services.

Promote robust levels of cybersecurity in e-government and e-commerce services through registration, standardisation, and certification, allowing people to transact online with confidence. The government and business should take efforts to promote trust in the secure use of their services. This is particularly important for public services, where, for example, trust in financial institutions would be undermined by poor security measures. Additionally, all ICT operators for e-commerce, e-transaction, and other similar activities, should be registered properly. The electronic system operators should be registered with MCIT, as stipulated in the Government regulation number 82/2012, and the business itself should be registered with relevant ministries. In the case of e-commerce, for example, as stated in Trade Law number 7/2014, the company should be registered with the Ministry of Trade. The Government decree for detail registration process is currently being prepared.

Therefore, it may be optimal for the government to establish e-government and e-commerce services in a secure environment through multi-stakeholder investment. The need for security for e-government and e-commerce services has been recognised by the stakeholders. Admittedly, registered services are usually considered more trusted than unregistered ones. A certified and standardised service is more trusted than an only registered one.

Recommendation #10: Develop a standard marketing strategy to promote privacy online for protecting personal data.

Laws and policies promoting access to government and other public information need to be considered, particularly regarding privacy and data protection. Currently, a privacy protection law is still being drafted, and the plan is to finalise it in 2017. For the moment, other laws, including ITE Law, the Government Regulation number 82/2012, Indonesian Civil Code (*KUH Perdata*), and other related laws are usually used for personal data protection. Also, ICT security standard and other measures are also socialized to promote data protection.

Therefore, it may be optimal for the government to promote a private online policy to access personal data collected and stored across government and other public institutions. The government and business should commit to protecting individual privacy and the personal information made available to the government and business when a user uses their services, such as e-government and e-commerce services. The online privacy policy should describe what information is made available to the government and business that provide electronic services to the society at large.

Recommendation #11: Identify a centre of excellence in cybersecurity research and education to locate strengths and providing focussed investment to address gaps.

The Ministry of Research, Technology and Higher Education (RISTEKDIKTI) should maintain and expand the cybersecurity education initiatives from reputable universities, such as ITB and UI, to offer a Master/Doctoral Degree in cybersecurity. This education should also include other subjects, such as law, politics, and related cyber security. The University appointed to be the centre of excellence should also develop technical capabilities to support other Universities, as well as private institutions.

Therefore, it may be optimal for the government to identify centres of excellence in cyber research and education across reputable public and private universities, as well as to establish a public-private partnership in education and training in cybersecurity.

Recommendation #12: Promote cybersecurity training and education programs designed for all employees at all levels in government organisations, state-owned enterprises, private critical infrastructure providers, and small-medium enterprises.

Universities should attempt to broaden the scope of their course and degree offering to include comprehensive cybersecurity issues, not just limited to information security. Also, primary and secondary schools should seek to implement security components to the IT literacy courses. The Ministry of Education, or another organisation, in cooperation with other stakeholders, should be responsible for the development and delivery of a national strategy in cyber education and manage the budget. This would ensure sustainable investment in cybersecurity education and research. The current program to provide scholarships for Indonesians to carry out ICT training at Professional Certification Institution (LSP TIK) should be expanded, and one of the programmes should be to promote cybersecurity skills. This can be followed by efforts to force any institution, starting with the government, to employ cybersecurity specialists operating ICT resources and infrastructures.

Therefore, it may be optimal for the government to promote incentives for cybersecurity training and education. It is important to engage with relevant stakeholders to ensure continuity the development of cybersecurity education, with funding dedicated to national research at universities.

Recommendation #13: Create a national-level register for information assurance and cyber security experts across the public and private sectors as a way of bringing new talent into the profession.

Job creation initiatives and structured cybersecurity training programmes for cybersecurity within and external to the organisation should be established and employers should be encouraged to train staff. As stipulated in the Government Regulation number 82/2012 whereby electronic system operators should employ Indonesian ICT experts, it can be used to ensure that ICT operators operate by the regulations. Hence, coordination among concerned multi-stakeholders should be realised to identify the available experts in the country.

Therefore, it may be optimal for the government to encourage employers to train staff and promote knowledge transfer from trained cybersecurity employees. In particular, it is essential to establish a national level register for trained cybersecurity employees in the country, so that job creation initiatives for cybersecurity within the organisation are well supported by Indonesian experts.

Recommendation #14: Raise awareness amongst senior government officials and board members of the critical national infrastructure operators of the cyber risks, and actions they can take to protect security-sensitive information.

Business leaders should collaborate to help prioritise what sorts of training are needed. Boards need to extend their awareness of cybersecurity issues to the point where they understand, generally, the threats faced by their business. Training should be provided to board members so that they can achieve such understanding. It is worth noting that a simulated attack can be carried out at a national, regional, or even government office level, to provide insight into cybersecurity. Hence, regulations concerning this simulation, similar to those on fire and earthquake drills, should be set up, as mentioned in recommendation #4.

Recommendation #15: Review existing legislation, for example, amending the ITE law No. 11/2008, to ensure that it remains relevant and effective in fighting cybercrime.

Amending the ITE law, or otherwise creating a unique substantive law for cybercrime, including outlining cooperation between ISPs and law enforcement, would enable the country to enhance its maturity in this field. Passing the draft amendments would be a step forward in enabling this. There also needs to be better harmonization of legislation between various types of laws to avoid confusion of authority. Regulations to be harmonised include mainly ITE Law number 11/08,

Telecommunications Law number 36/99, Broadcasting Law number 32/02, and the Press Law number 40/99.

Therefore, it may be optimal for the government to establish a comprehensive ICT security legislative and regulatory framework addressing cybersecurity, by strengthening the position of the government regulation number 82/2012 in the digital environment. Additionally, passing a unique data protection legislation that designates the responsible body for monitoring the implementation of such legislation would better protect user privacy. These steps are crucial for achieving the established stage of maturity in legislation.

Recommendation #16: Strengthen law enforcement and prosecutors' capabilities to investigate cybercrime and bring those responsible to justice.

There needs to be better clarification of roles and responsibilities of law enforcement and civil investigative capacities. This provides a clear point of contact for the private sector and civil-society actors to cooperate with. Local law enforcement capacity also needs to be further enhanced to ensure an investigation is possible at the provincial and district levels. Finally, additional training needs to be provided to prosecution and judicial actors to ensure that, once investigations have been conducted, the prosecution can utilize digital evidence to achieve an accurate verdict.

Therefore, it may be optimal for the government to establish a comprehensive institutional capacity to investigate and manage cybercrime cases, including human, procedural and technological resources, full investigate measures, digital chain of custody and evidence integrity management, ability to attend criminal proceedings in person, and make formal collaboration mechanisms with multiple national and international stakeholders. Also, it is worth developing sufficient judicial resources and training to ensure effective and efficient prosecution of cybercrime and electronic evidence cases.

Recommendation #17: Create a single reporting system for electronic system operators for public services to report and disclose cybercrime incidents and data breaches, so that action can be taken.

Responsible disclosure frameworks should be clearly communicated, and include a disclosure deadline, scheduled resolution, and an acknowledgement report. The body responsible for collecting this information needs to have the capacity to share technical details of the incident to a broad range of stakeholders.

Therefore, it may be optimal for the government to establish a vulnerability disclosure framework, requiring electronic system operators to disclose cybercrime incidents and data breaches, so that such actions can be taken.

Recommendation #18: Promote cybersecurity requirements in government procurement processes for managing the national cyber defence.

Some implementation of cyber security standards, such as ISO/IEC 27001, has been carried out, but only minimal acceptance practices have been done in IT products and services during the procurement process. Identifying national cyber risk during procurement or software development, especially for CNIs, is an essential issue to be considered during the development of a National Cyber Security Strategy in Indonesia. For example, as stated in the Government Regulation number 82/2012, a source code has to be surrendered to the Government during the software procurement. This may cause some problems should the company providing the software not agree with this. In this case, the Government should also consider the development of local capabilities to enable them to produce enterprise application software for CNIs and/or public services or national security ministries and agencies. This initiative may need the support of local research centres and universities.

Therefore, it may be optimal for the government to develop cybersecurity requirements and standards in the public procurement practices and procedures, especially if the contracts involve handling government security-sensitive information and provisions of certain IT products and services.

Recommendation #19: Establish a unit under the related government ministry to formally monitor and control national infrastructure to help ensure Indonesia's security and resilience.

More formal management of national infrastructure, including documenting roles and responsibilities, will aid in the currently ad-hoc nature of resilience efforts in infrastructure. Also, it is necessary to promote technologies and processes deployed to meet international IT standards, guidelines, and best practices. It is also important to establish roles and responsibilities to formally manage national infrastructures, such as telecommunications and Internet. For example, the UK Government established the Centre for the Protection of National Infrastructure (CPNI) to provide protective security advice across the UK's critical national infrastructure, as well as to help ensure the UK's security and resilience.

Therefore, it may be optimal for the government to establish centres for national infrastructure resilience to safeguard the public's way of life through building a more secure and resilient national infrastructure, by providing protective cybersecurity advice, as well as implementing standards, guidelines, and best practices within the national infrastructure. It is worth noting that developing the country's independent resilience is required.

Recommendation #20: Provide incentive-based cybersecurity solutions for local cybersecurity products or the cyber insurance marketplace.

Providing incentives for the local cybersecurity technology marketplace with bespoke security offerings would help capacity in this area. This could capitalise from the existing cryptographic efforts being made at the ministerial level. Therefore, it may be optimal for the government to encourage local providers to produce cybersecurity non-specialised products and services, as well as to develop the need for a market in cybercrime insurance through the assessment of financial risks for public and private sectors.

Based on the above recommendations, and given the current situation, it seems that priorities should be set up. The cybersecurity capacity-building initiatives should be conducted in an environmentally sustainable manner, meaning that the cybersecurity initiatives should not depend on the senior officials who currently lead the country or government ministries. A key issue is that the government needs to be aware of whether they have security-sensitive data processed, transmitted, and stored in cyberspace. Also, the government should be aware that information technology products and services become increasingly integrated with physical infrastructures, as well as cyberspace, which is difficult to secure, as they are vulnerable to a wide range of risk, stemming from both physical and cyber threats. If this is the case, then the government should develop cybersecurity requirements that are agreed upon with key national stakeholders, and have to be met by the government agencies, businesses, and civil society. It is worth noting that Indonesian community awareness on physical infrastructure operations is quite high. It can be seen that almost all houses in Indonesia are protected by high fences. Lamps to lighten streets and outside parts of the houses are quite common, and security guards are employed by nearly all government agencies, businesses areas, and other places that are considered important according to their value or “criticality”. However, that is not yet the case in cyberspace, as the Government is not as reliant on the Internet and digital environment. Thus, it is important into give a clear understanding of how to convert this simple formula into action on Cyberspace.

In conclusion, the Government should take into consideration some of the recommendations lists above. While the adoption of these recommendations will depend on the national objectives and priorities, embracing some of these recommendations will hopefully improve the overall state of cybersecurity capacity in the country. The Global Cyber Security Capacity Centre hopes to continue its engagement with MCIT and Telkom University moving forward.

Appendix: Recommendations for Cybersecurity Capacity

Dimension	Capacity	Stage of Maturity		Proposed Actions to include	Responsible Agency
		Current	Future		
Cybersecurity Policy and Strategy	Documented National Cyber Security Strategy	Start-up - Formative	Established	1. Build a national cybersecurity strategy based on government consultation with key stakeholders groups 2. Develop a better understanding of national cybersecurity risks and threat to drive cybersecurity capacity building at a national level 3. Create a single cybersecurity programme within each government entity, with goals, milestones, and metrics defined to measure progress. 4. Create clear and agreed upon roles and responsibilities for cybersecurity functions within government entities. 5. Ensure that the national cyber security strategy is linked explicitly to national risks, and priorities include public awareness raising, mitigation of cyber-crime, incident response capability, and critical national infrastructure protection.	POLHUKAM

	Incident Response	Formative	Established	1. Build a central registry of national-level cyber incidents. 2. Develop a routine and coordinated relationship between the public and private sectors for the basic function of national level incident responses. 3. Establish a coordinated national incident response, with clear processes and defined roles and responsibilities, including lines of communications for the crisis.	KOMINFO
	CNI Protection	Start-up to Formative	Established	1. Create a formal list of CNI assets with identified risk-based priorities through government consultation with the major national stakeholders. 2. Implement an audit of CNI assets on a regular basis, and discuss dissemination of CNI asset audit list with relevant stakeholders. 3. Establish a mechanism for regular vulnerability disclosure between the public and private sectors, including the scope of reporting requirements.	KOMINFO + KEMHAN

				4. Define reporting requirements between CNI asset owners and the public sector to address national security needs. 5. Establish information protection procedures and processes of critical assets with adequate technical solutions. 6. Create a response plan and produce a repeatable course of action in the event of an incident. 7. Develop a regular dialogue between tactical and executive strategic levels regarding cyber risk practices. 8. Establish formal internal and external CNI communication strategies across sectors, with an endorsed communication strategy and clear point of contact. 9. Establish minimum-security measures and guidelines for CNI cyber best practice, with the implementation of CNI standards monitored and reviewed on a regular basis.	

	Crisis Management	Start-up to Formative	Established	1. Establish general awareness of crisis management technique and goals across stakeholders. 2. Create a crisis management protocol or procedure document, with relevant stakeholders included in the evaluation process. 3. Implement crisis management exercises at the national level, with results feeding into decision-making.	KOMINFO
	Cyber Defence Consideration	Start-up to Formative	Established	1. Create a national cyber defence policy and strategy, including the military's position on its response to different types and levels of cyber attacks, aimed at national infrastructure resilience. 2. Establish a central command and control structure through a cyber defence operation unit that is incorporated into different branches of the armed forces. 3. Create and build a dedicated and integrated civilian and military capability within a	KEMHAN

				defined organisation of the Ministry of Defence. 4. Develop cyber defence capability requirements that are agreed upon between the public and private sectors to minimize the threat to national security 5. Develop a cyber defence coordination protocol in response to malicious attacks on the military information system and critical national infrastructure.	
	Digital Redundancy	Formative-Established	Established	1. Establish emergency response asset priorities and standard operating procedures in the event of a communication disruption. 2. Implement appropriate resources to hardware integration, technology stress testing, and personnel training and crisis simulation drills in the case of a communication disruption. 3. Develop communication scenarios and exercises that are distributed across emergency response function, geographic	KOMINFO

				areas of responsibility, public and private responders, and command authorities.	
Cyber Culture and Society	Cybersecurity Mindset	Start-up - Formative	Established	1. Promote greater levels of cybersecurity best practices across government at all levels 2. Promote greater levels of cyber security mindset across business and industry 3. Promote consistent levels of cyber security mindset across society at large through programmes and materials that are available publicly to train and improve cybersecurity practices 4. Develop societal consciousness of the secure use of online systems to manage their privacy online and protect themselves from intrusion, interference, or unwanted access to information by others.	KOMINFO
	Cybersecurity Awareness	Formative	Established	1. Establish national awareness-raising campaigns, closely linked to cyber security strategy, with defined targets, covering all	KOMINFO

				groups and coordination or measurement efforts. 2. Develop a single online portal through multi-stakeholder engagement in delivery of awareness raising services and products.	
	Confidence and Trust on the Internet	Formative	Established	1. Promote greater levels of trust in online services with measurement efforts 2. Establish a coordinated national program to promote trust in online services, with budget allocation for security measures 3. Promote greater levels of security measures to promote trust in e-government services, in which all breaches are reported, identified and acknowledgement. 4. Promote greater levels of compliance to Internet and web standard to protect the anonymity of users 5. Establish e-commerce services in a secure environment through multiple stakeholders' investments with privacy	KOMINFO

				policies created and set up to protect personal information from unauthorised disclosure	
	Privacy Online	Start-up	Formative	1. Promote a privacy policy and privacy standard to access personal data collected and stored across government and other public institutions. 2. Develop a better understanding of privacy in the workplace through employee programs, as it is an important component of cyber security	KOMINFO
Cybersecurity Education, Training, and Skills	National Availability of Cyber Education and Training	Formative	Established	1. Identify Centres of Excellence in cyber research and education across reputable public and private universities 2. Establish education programs in cyber security at the national and institutional levels, ranging from primary to post-graduate levels, including vocational education in modular form 3. Encourage stakeholders to invest in cyber security training across a full range of employees, including executive and management levels.	RISTEKDIKTI

				4. Establish public-private partnership in education and training. 5. Develop metrics to assess the effectiveness of models and procedures for cyber security training 6. Promote greater levels of accreditation to cyber security professionals, with a list of certified cyber security professionals	
	National Development of Cyber Security Education	Start-up	Formative	1. Promote incentives for cyber security training and education 2. Establish an office within the related Ministry for the development and delivery of cyber security programme, with budget lines for training and research and development in cyber security. 3. Engage with relevant stakeholders to ensure continuity of the development of cyber security education, with funding dedicated to national research at universities.	RISETDIKTI
	Training and Educational Initiatives within Public and Private Sector	Formative	Established	1. Encourage employers to train staff and promote knowledge	KOMINFO

				transfer from trained cybersecurity employees. 2. Establish job creation initiatives for cyber security within the organisation. 3. Develop structured cybersecurity training programs to specify precise roles and responsibilities within the public and private sectors	
	Corporate Governance, Knowledge and Standards.	Start-up - Formative	Formative	1. Raise awareness of cyber security issues amongst boards 2. Establish a training program in cyber security for board members	KOMINFO + BUMN
Legal and Regulatory Framework	Cybersecurity Legal Framework	Formative - Establish	Established	1. Establish a comprehensive ICT security legislative and regulatory framework addressing cyber security, including legislation protecting the rights of individuals and organisations in the digital environment. 2. Establish comprehensive data protection legislation and regulatory procedures that recognise fundamental human and civil rights, including domestic laws providing for the	KOMINFO

				individual's right to privacy specifying notice, purpose, consent, security, disclosure, access, and accountability of personal information. 3. Review existing legislation to ensure that it criminalised a variety of computer-related crimes that may be covered in a specific legislation or addressed in the criminal code. 4. Establish a comprehensive criminal law with procedural powers for investigation of cybercrime and evidentiary requirements to deter, respond to, and prosecute cybercrime, with best practices applied by law enforcement in exercising procedural powers	
	Legal Investigation	Formative	Established	1. Establish a comprehensive institutional capacity to investigate and manage cybercrime cases, including human, procedural, and technological resources, full investigative measures, a digital chain of custody and evidence integrity management, the	POLRI+ KOMINFO

				ability to attend criminal proceedings in person, and formal collaboration mechanisms with multiple national and international stakeholders. 2. Establish institutional capacity to prosecute and handle cybercrime cases involving electronic evidence, with sufficient human training and technological resources. 3. Establish formal mechanisms of international cooperation to prevent and combat cybercrime 4. Create sufficient judicial resources and training to ensure effective and efficient prosecution of cybercrime and electronic evidence cases, with formal collaboration mechanisms with multiple international counterparts.	
	Responsibility Reporting	Start-up – Formative	Formative	1. Establish a vulnerability disclosure framework that includes a disclosure deadline, schedules resolution, and an acknowledgement report.	KOMINFO

				2. Encourage organisations to share technical details of the vulnerability with other stakeholders, who can distribute the information more broadly	
Standard, Organisation and Technologies	Adherence to Standards	Start-up - Formative	Established	1. Establish a nationally agreed upon baseline of cyber security related standards that are widely adopted across the public sector and CNI organisations 2. Promote the use of standards to mitigate CNI supply systems risk, with measurement efforts and oversight from the government. 3. Develop cyber security standards in the procurement practices and procedures, with measurement and quality assessments of process effectiveness 4. Promote an established programme for promoting standards adoption in software development across public and private sector systems, which includes tracking of standards compliance, high integrity system, and software development techniques.	KOMINFO + BSN

	National Infrastructure Resilience	Formative	Established	1. Promote technology and processes, deployed to meet international IT standards, guidelines, and best practices 2. Support the use of the Internet for communication between all stakeholders, integrated into everyday operating practice 3. Establish processes and measures for the Internet that are used for business e-commerce and electronic transactions and authentication. 4. Establish roles and responsibilities to formally manage national infrastructure, with documented processes.	KOMINFO + KEMHAN
	Cybersecurity Marketplace	Start-up	Formative	1. Promote security technology and processes in government and the private sector. 2. Encourage local providers to produce cyber security non-specialised products and services. 3. Identify the need for a market in cybercrime insurance through the assessment of financial risks for the public and private sectors.	KOMINFO + LEMSANEG