GLOBAL PARTNERS DIGITAL

November 2016

Mapping the Cyber Policy Landscape: Indonesia

WRITTEN BY **LEONARDUS K. NUGRAHA AND DINITA A. PUTRI**

Global Partners Digital
Second Home
68 - 80 Hanbury Street
London
E1 5JL
+44 (0)203 818 3258
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Designed by SoapBox
Typeset by Jonathan Jacobs
Cover image adapted from David Nagy under Creative Commons Licence 2.0.
https://www.flickr.com/photos/ndave/

Company Nº 520 1603
VAT Nº 840 1912 54

GLOBAL PARTNERS DIGITAL

Mapping the Cyber Policy Landscape: Indonesia

WRITTEN BY LEONARDUS K NUGRAHA AND DINITA A PUTRI

gp-digital.org

This report was prepared by Leonardus K. Nugraha and Dinita A. Putri, with contributions from Maharani Karlina and Pravitha Lascaria Utami on analysis of regulations and actors.

The team is grateful for guidance received from Shita Laksmi as an advisor, transcription from Syari Puspita, and assistance with the report's layout from Mona Luthfina.

Throughout the research, the team was privileged to have the support of several individuals who participated in the study through the interview process. The team would particularly like to thank Donny B.U and Wahyudi Djafar for their generous support and insights during both formal and informal discussions.

The research was commissioned by Global Partners Digital, and undertaken by the Centre for Innovation Policy and Governance (CIPG), Jakarta.

CONTENTS

ABBREVIATIONS

AJI	Aliansi Jurnalis Independen / Independent Journalists' Association
APCERT	Asia Pacific Computer Emergency Response Team
APJII	Asosiasi Penyelenggara Jasa Internet Indonesia / Indonesian Internet Providers Association
BCN	Badan Cyber Nasional / National Cyber Agency
BIN	Badan Intelijen Negara / State Intelligence Agency
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CSO	Civil Society Organisation
ICT	Information and Communications Technology
IGF	Internet Governance Forum
ITE	Internet and Electronic Transaction
KAMI	Keamanan Informasi / Information Security
Lemsaneg	Lembaga Sandi Negara / National Encryption Agency
MCIT	Ministry of Communications and Informatics
Kemenkumham	Kementerian Hukum dan Hak Asasi Manusia / Law and Human Rights Ministry
Kemenkopolhukam	Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan / Coordinating Political, Legal and Security Affairs Ministry
MoD	Ministry of Defense
MoFA	Ministry of Foreign Affairs
MoHA	Ministry of Home Affairs

Perpres	Peraturan Presiden / Presidential Regulation
Polri	Kepolisian Negara Republik Indonesia / Indonesian National Police
PP	Peraturan Pemerintah / Government Regulation
SAFENET	Southeast Asia Freedom of Expression Network
SKKNI	Standar Kompetensi Kerja Nasional Indonesia / National Working Competency Standards
Warnet	Warung Internet / Internet Cafe

01

BACKGROUND

In most countries, there is convincing evidence that Information and Communication Technology (ICT) has contributed positively to economic development and growth. This includes Indonesia, where the exponential growth of internet users and increasing middle class weatlh, among other factors, have played an important role in the growth of Indonesia's e-commerce market. Recently, the Internet Service Providers Association predicted that in 2016, the e-commerce market would reach Rp 25 trillion, with 49 million consumers. The figures are up from IDR 18 trillion (US$ 1.3 billion) with 37 million consumers in 2015 and IDR 12 trillion with 27 million consumers in 2014[1]. While Indonesian e-commerce is one of the most prominent issues in discussions around Southeast Asia's startup culture, online sales still only account for less than one percent of the nation's entire retail sector.

According to Internet Live Stats, Indonesia has 53,236,179 internet users - the 12th largest population of active internet users in the world. In terms of social media activities, Indonesia is considered highly connected and active. Today, Indonesia has the 4th largest Facebook user base and the 5th largest Twitter user base in the world. Combined with the growth of the e-commerce market, these numbers alone are sufficient to highlight the importance of ICT sector in Indonesia.

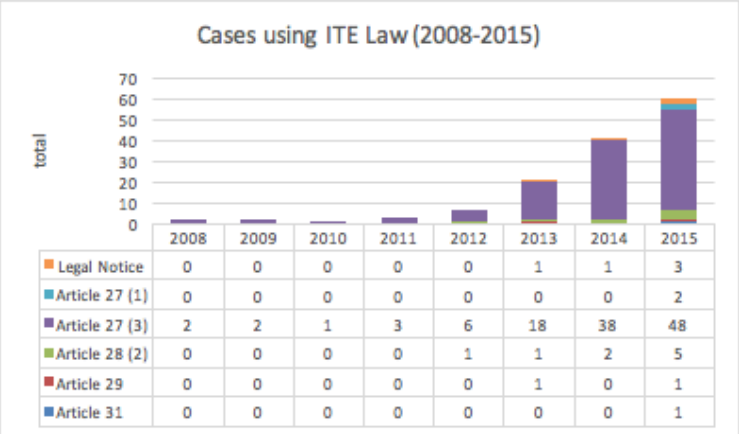
A growing reliance on ICTs also poses an increase in risk - evoking the old truism that technology can be both enabling and threatening. Having a comprehensive system that protects both users and information is therefore important. However, governing the cyber world can be perplexing. The question of who should govern it, and how they should do so, still remains. In terms of cybersecurity, Indonesia is ranked the second most vulnerable country for cyber-attacks [2]. Based on the data from Ministry of Communication and Informatics, there have been 36.6 million attacks on internet networks in Indonesia in just the past three years. This vulnerability is caused by several issues hindering the ideal practice of cyber governance, such as a lack of coordination between actors in cybersecurity. The unprecedented freedom of information and data raises the question of who will be responsible for governing it, and protecting the safety of citizens.

The country faces numerous challenges in developing its cybersecurity system, particularly in finding the proper mechanism to coordinate across various ministries, agencies, and sub-national governments. The system and mechanism which would decide roles and responsibilities is still being fiercely debated. This has meant that citizens in Indonesia receive very little protection from the government regarding cybersecurity. From the citizen viewpoint, there is still a low level of public awareness in terms of citizen rights and data privacy. The difficulty lies in finding the connection between the issue of privacy and other issues, so that it can become a 'common' and important issue. Furthermore,

1. See http://www.thejakartapost.com/news/2016/01/27/e-commerce-be-new-driver-growth-adb.html, accessed 27 June 2016.
2. See http://www.opengovasia.com/articles/6563-indonesia-launches-cyber-security-agency-in-wake-of-growing-threat-landscape, accessed 22 June 2016.

civil society advocacy for privacy issue has been somewhat scattered, with each organisation having its own agenda.

Indonesia is still in the process of drafting the ministry's regulation on private data protection in electronic systems, as well as the draft for personal data protection. It is understood that the regulation on cyber policy, including cybersecurity, needs to be aligned with other regulations - such as the Telecommunication Law, the Anti-Terrorism Law, the Law on State Intelligence, and a number of other acts. Currently, the most relevant regulations related to cyber cases are the Telecommunication Law and Internet and Electronic Transaction Law. However, these regulations are seen as ambiguous in providing safeguards for freedom of expression within the borders of ethics and tolerance. In fact, the number of cases using the Internet and Electronic Transaction (ITE) Law on the internet – mostly related to criminal defamation – has been rising for the last few years (See Figure 1). This situation highlights the need to review the existing regulations, as well as provide a more comprehensive set of regulations and mechanisms to internalise human rights principles in cyber governance.



	2008	2009	2010	2011	2012	2013	2014	2015
Legal Notice	0	0	0	0	0	1	1	3
Article 27 (1)	0	0	0	0	0	0	0	2
Article 27 (3)	2	2	1	3	6	18	38	48
Article 28 (2)	0	0	0	0	1	1	2	5
Article 29	0	0	0	0	0	1	0	1
Article 31	0	0	0	0	0	0	0	1

Figure 1. Cases using ITE Law from 2008 – 2015
Source: SAFENET (2016)

In June 2016, there was a cyber attack on the Central Bank of Indonesia website and several other central banks in Asia. The banking sector is one of the most advanced sectors in terms of cyber protection – and in this instance, no money was lost. There is usually cooperation between central banks, through which they share experience on cyber attacks. The private sector is also seen as more advanced in terms of cybersecurity governance. Government should cooperate closely with the private sector, especially in terms of providing resources for cybersecurity governance.

Apart from dealing with ICT-related cases, the government is in the process of establishing a National Cyber Agency, where it is expected to strengthen cybersecurity protection in Indonesia. There are also plans to bring the National Encryption Agency and the Ministry of Communication and Informatics – among institutions – on board.

In order to study cyber policy and inform the multistakeholder framework in national policymaking processes, it is necessary to identify relevant actors, pressing issues and existing instruments within the cyber policy landscape in Indonesia. Therefore, this study will map the cyber policy landscape, identify gaps and provide recommendations on how to fill these gaps and develop the needed capacities in Indonesia.

Objectives, RQs and research undertaken

The purpose of this study is to map the cyber policy landscape in Indonesia. This will cover the relevant actors, interactions between actors, existing regulations and the interrelation between regulations. Specifically, this scoping study will cover the following questions:

1. What is the cybersecurity policy trajectory in Indonesia? How does the policymaking process take place and how does this affect the dynamics of cybersecurity and internet governance in Indonesia?

2. Which actors are involved in the dynamics of the policymaking processes? How do we understand the link between actors and the regulatory process with regards to cybersecurity in Indonesia? How and why do different actors affect regulatory rationales and the dynamics of the policymaking processes?

To answer these questions, a combination of methods and research instruments were used, combining secondary data collection (i.e. desk research to map relevant actors and existing regulations with regard to cybersecurity) and primary data gathering (i.e. expert interviews conducted to identify factors influencing policymaking and understand the links between actors in response to the second question).

Our secondary data sources consist of papers, popular articles, presentations, book chapters and grey literature. To gain a more detailed and nuanced understanding on how the cybersecurity policymaking process takes place, we conducted text analysis, using legal documents, annual reports, online and printed articles. Subsequently, we sourced legal and regulatory information mostly from online ministerial websites, particularly from the Ministry of Communication and Informatics and the Ministry of Law and Human Rights. We also gathered data from several annual ministerial and state agency reports.

We also gathered data from mainstream media articles, such as Kompas, Tempo, CNN, detik.com, The Jakarta Post, Liputan 6 and National Geographic. This data ranges from 2011 to 2016. We also used specific data from related CSO reports such as SAFENET, AJI, Elsam and ICT Watch. This data collection was mainly used to capture the big picture of cyber governance and particularly the extent to which the dynamics of its actors characterised the policymaking processes.

Meanwhile, the primary data was collected by conducting in-depth interviews with representatives from government actors, the private sector, civil society and academia. In this endeavour, we encountered several methodological challenges. Firstly, the lack of standard practice in Indonesia for recording research data. We responded to this limitation by using official data when available and updating them with other sources when possible. Secondly, concerning interviews, issues around confidentiality. While actors were relatively open to discuss various relevant topics, due to their importance, some respondents were reluctant to provide full disclosure on other topics. In response, we offered the option of anonymity to respondents who did not wish to be identified. Therefore, for certain topics that are too sensitive to be discussed, we tried to complement the information with secondary data.

02

CYBERSECURITY ACTORS IN INDONESIA

> *When local governments suffered from cyber attack, [there are] only two questions they are thinking about. First, whether the incident is [a] cyber attack or not. Second, which authority [is] responsible to provide help and assistance, and how [can I] contact them."*

(Undisclosed, Academic, Interview, July 2016)

Looking at the different aspects of cybersecurity, it can sometimes seem as if everyone is a stakeholder. Cybersecurity is relevant not only to government actors or private networks, but also to personal data and privacy. However, since the development of cybersecurity in Indonesia remains sporadic, each institution usually develops their own CERTs/CSIRTs. The establishment of internal CERTs/CSIRTs in each institution is authorized as a means of preventing and responding to cyber attacks – as long as the attack is not classified as a national threat.

There are several notable actors involved in cybersecurity governance in Indonesia. We divided actors based on their approach towards cybersecurity, into five categories: (1) Government; (2) Private sector; (3) Civil society; (4) Academia; and (5) Technical communities. Within each category, there are several institutions deemed responsible - although it is also possible for one institution to cover more than one specific issue or approach. These divisions are made based on our observation of the work of each actor. It is important to note, however, that in certain cases some actors are performing more than one role in cybersecurity governance. For example, several academics are also part of civil society and/or technical communities due to their competencies on several topics.

The map on the next page shows the different perspectives through which actors see cybersecurity governance[1]. At the same time, it does not intend to imply that one actor has greater authority than another. Each organisation has its own function and mandate, with every actor, agency or ministry possessing its own understanding of cybersecurity governance – which is not always as rigid as it may seem. Despite the many different approaches to cybersecurity governance, it is often still performed in individual silos. However, most actors are open to discussions on major issues related to cybersecurity.

1. The foundation of this reasoning is based on text analysis how these actors reacted to cybersecurity-related issues in mass media, also on panel judgement.

Figure 2. Actors and their approaches to cybersecurity in Indonesia. Source: authors

In Indonesia, general understanding of cybersecurity remains very low. Most actors, including the government and private sector, still focus on the 'detection' level.[2] Although some cyber attack cases have shown that Indonesia is moving to the 'response' level, a reactive rather than proactive approach is still the norm. Cybersecurity does not seem to be the main focus in terms of data protection as well as defense in Indonesia. Despite the number of threats that have been recorded during the last three years, Indonesia has yet to update its cybersecurity management. The quote from public administration at the beginning of this chapter demonstrates the lack of awareness of cybersecurity and it unexpectedly comes from actors involved in public administrations. This marks one of the challenges in developing national cybersecurity capabilites, especially when coordinating across a large and diffuse government (Djafar 2016).

We outline the profile and activity of each of the defined actors below.

Government

Approaches of government institutions towards cybersecurity mostly focus on national threats and the protection of critical national infrastructure. As mentioned above, there are two ministries currently responsible for managing cybersecurity

2. See http://nationalgeographic.co.id/berita/2016/04/soal-keamanan-dunia-maya-indonesia-masih-jadi-korban-bully, accessed 14 July 2016.

in Indonesia: the Coordinating Ministry of Politics, Law, and Security; and the Ministry of Communication and Technology. Other than these two ministries, the Indonesia Armed Force, National Intelligence Agency, Ministry of Foreign Affairs, and the latest is the National Encryption Agency also contribute to discussions around cybersecurity.

The Ministry of Communication and Information Technology (MCIT) responded to the need for an internet security strategy by establishing ID-SIRTII in 2007. ID-SIRTII's main task is to perform monitoring, maintain early warning and detection systems for threats in telecommunication networks, and deal with legal action on cybersecurity disputes. ID-SIRTII is also responsible for creating a secure environment for internet-based communications within the country, and serving as a coordination centre for issues related to cybersecurity. In 2010, the MCIT established the Directorate of Information Security to assist the ministry in formulating and implementing policies related to cybersecurity, along with establishing norms, standards, procedures and criteria in the area of information security. The Directorate of Information Security is incorporated inside the MCIT structure, while ID-SIRTII acts as an independent state body.

The Coordinating Ministry of Politics, Law, and Security also has its own cybersecurity desk, which aims to handle and manage national cybersecurity threats. If the MCIT is the lead institution regarding civil cybersecurity, the Coordinating Ministry of Politics, Law, and Security is responsible for national security-related threats. Several months ago, this cyber desk initiated a Cybersecurity Forum – an informal group to discuss issues related to cyber attacks and cyber governance. This informal group consists of cybercrime actors - from business representatives, to police departments and civil society organisations.

The National Encryption Agency is another important actor which has started to engage in cybersecurity discussions in Indonesia. They have their own version of cyber governance and could come to lead the coordination of cybersecurity in Indonesia.

"[in terms of cybersecurity governance] Lemsaneg (National Encryption Agency) has its own version… [they are] offering to become the operational agency [for cybersecurity governance]. So they are currently developing a new Presidential Decree [on cybersecurity governance]". (Undisclosed, Civil Society, Interview, June 2016)

There is a division of approach among government institutions. Institutions closely related to law enforcement usually focus more on cybercrime issues, while those related to military forces usually focus on cyber espionage and cyber terrorism.

Despite having a similar approach to cybersecurity, these government actors still possess their own mechanisms for dealing with cyber attacks. The nonexistence of a coordination agency is one of the reasons why these actors perform in silos.

Private sector

In terms of technological development, the private sector is almost always more advanced than the government and civil society. This is similarly true of cybersecurity governance. In Indonesia, the business sector is often seen to be more active in the discussion of cyber policy and cyber management.

The approach of the business sector towards cybersecurity seems fairly clear. Their main interest, first and foremost, is to protect infrastructure and business development.

"If you talk about cybersecurity, don't only talk about cyber war… It does not

always relate to cyber war. This [cybersecurity] also relates to our [private sector] infrastructure security, transaction safety, network security and so on… how our critical infrastructure is well protected." (Undisclosed, Private Sector, Interview, July 2016)

It is not surprising that the business sector has established an advanced and well developed CSIRT/CERT for cybersecurity. In terms of regulation, the private sector mostly uses ITE Law and Telecommunication Law as the basis for developing tools for cyber attack prevention. However, it is also notable that several regulations are urgently needed to protect business sector interests, such as OTT regulation and data privacy regulation – both of which are still in the early stage of initiation.

The private sector has a fairly good knowledge of cybersecurity because it has the resources to develop the necessary tools and systems needed for cyber protection. However, our observations show that despite their knowledge and resources, helping the government develop good cybersecurity mechanisms is not their main priority. The involvement of the private sector in policy discussions does not, therefore, guarantee their participation in increasing the government's capacity and capability in governing cybersecurity. Although capacity and capability building is not mainly the responsibility of the private sector, they do have good resources, and their participation would greatly benefit cybersecurity governance in Indonesia.

Civil society and academia

In cybersecurity discussions, civil society seems to be lagging behind – notably on the issues of privacy and personal data protection. Our observations show only a few communities actively involved in cybersecurity issues, with most are taking a human rights approach.

According to Budi Rahardjo, founder of ID-CERT, civil society and academicia can contribute to cybersecurity by increasing security awareness and building a security culture, making up for the limitations of the public and private sectors (DAKA 2013). In line with this vision, several actors are working to fill this gap. Cases related to online child protection, for example, show how academia and civil society can contribute to cybersecurity governance. Since Indonesia does not have any officially recognised agency offering institutional support on child online protection, these actors provide an avenue for the treatment of incidents related to child online protection. One of them is ICT Watch with their "Internet Sehat" (Healthy Internet) program[3] . Through the program, ICT Watch has endeavoured to show that people can take responsibility for their online activities - from creating modules for parents and teachers, to publishing comic books for children/youngsters on internet safety and encouraging people to participate in various online and offline activities.

As with the government, civil society organisations often approach cybersecurity from different perspectives. For example, the human rights organisation Elsam uses a freedom of expression approach, while ICT Watch uses a more technological approach. CSIS is a new civil society actor which uses a digital economy and national security approach. These different basic principles then lead to different priorities which complement one another.

Technical communities

Indonesia has several CERTs and critical security incident response teams (CSIRTs) organised by both the government and the private sector. Among those teams, the most frequently mentioned are ID-CERT and ID-SIRTII/CC due to their respective roles and history. ID-CERT (http://cert.id/) is the first computer emergency response team in Indonesia. Established in 1998 by Budi Rahardjo, ID-CERT is a community-based team for independent technical coordination. It is one of the

3. ICT Watch was selected for a 2016 WSIS Champion Projects Award for their project. ICT Watch's project was selected under the "Ethical Dimensions of the Information Society" subcategory, based on over 245, 000 votes, as well as a selection phase conducted by WSIS's Expert Group. See http://groups.itu.int/stocktaking/WSISPrizes/WSISPrizes2016.aspx#champion-projects, accessed 20 July 2016

founders of APCERT forum (Asia Pacific Computer Emergency Response Team). The Indonesia Security Incident Response Team of the Internet Infrastructure Coordination Center (ID-SIRTII/CC) is Indonesia's national incident response team. Established in 2003 by eight stakeholders from various sectors , the Center[4] is the point of contact for domestic and international CERTs. As a member of FIRST, APCERT and OIC-CERT, ID-SIRTII/CC is closely engaged in regional drills, workshops and meetings, and runs a strong domestic program of training workshops for government and private sector ICT workers (ASPI 2015).

Apart from the abovementioned computer emergency response teams, there are at least 14 other CERTs/CSIRTs in Indonesia[5]. The list is as follows:

No.	CERTs/CSIRTs	Function	Website
1.	ID-CERT	Public	http://cert.id/
2.	ID-SIRTII/CC	Public	http://idsirtii.or.id/
3.	Jabar-CSIRT	Region-based	
4.	JabarAcad-CSIRT	Region-based	
5.	JabarProv-CSIRT	Region-based	
6.	Jatim-CSIRT	Region-based	
7.	JogjaPG-CSIRT	Region-based	
8.	AcadCSIRT	Sector-based	http://acad-csirt.or.id/
9.	ID.GovCSIRT	Sector-based	http://govcsirt.kominfo.go.id/
10.	BPPT-CSIRT	Internal CSIRT	https://csirt.bppt.go.id/
11.	CSOC-Telkom	Internal CSIRT	
12.	IT security Mandiri team	Internal CSIRT	
13.	XL-CSIRT	Internal CSIRT	
14.	National Defense sector	CSIRT-similar function	
15.	Pustekkom, Ministry of Education and Culture	CSIRT-similar function	
16.	Directorate of Trade Security, Ministry of Trade	CSIRT-similar function	

Table 1. List of CERTs/CSIRTs in Indonesia
Source: ID-CERT (2016)

In contrast to ID-CERT and ID-SIRTII/CC, these CERTs/CSIRTs are closed CERTs/CSIRTs, with some serving limited groups or communities and bound to certain geographical territories.

Summary

From this mapping of cybersecurity actors, we found two distinct 'wings': one which leans towards human rights perspectives, and one heavily influenced by the perspective of state defence. In general, the latter utilises rigid arguments in the debate, with some of them resting on faulty premises. This study also observed that those with a defence perspective tend to be more cautious than those with a human rights perspective.

In terms of national cybersecurity governance, each of the main actors above seem to understand that there needs to be a coordinating agency to manage the diverse understandings of cybersecurity. However, the tone of the debate is currently very heated, despite its complexity. It remains to be seen whether Indonesia will encourage one unit of its security structure to manage cybersecurity across the government, or develop a coordinating body to allow agencies to manage their own networks autonomously, with coordination when needed.

4. The first stakeholders of ID-SIRTII/CC are MCIT, the National Police, Attorney General's Office, Bank of Indonesia, APJII, Association of the Internet kiosk, Association of Indonesia Credit Card and Mastel. See http://idsirtii.or.id/halaman/tentang/sejarah-id-sirtii-cc.html, accessed 15 September 2016.
5. See http://www.cert.or.id/index-berita/id/berita/65/, accessed 20 September 2016.

03

CYBERSECURITY POLICY IN INDONESIA: AN OVERVIEW

> *At least one thing is obvious: the government is always late to anticipate [new issue regarding technology] . The way they release policies on handling Pokemon Go is too much [heavy- handed]. So, they tend to be reactive, and too often late. The process is slow, that's for sure. Some Permen [Ministerial Regulation] take years just to get released. So more speed is indeed crucial, since the advancement of technology will only get faster than the latest policy.*

(Undisclosed, Academia, Interview, July 2016)

The advent of the 1998 Reformasi marks a major turning point in the history of media in Indonesia. The changing media landscape, together with the advancement of technological innovations created the need for regulation in the sector. However, the policies which emerged did not understand the context in which the new technology works, and subsequently failed to anticipate its consequences. In the same way, the rapid proliferation of the internet is not always addressed by policy in an appropriate manner. One of the new challenges to the wider deployment of this new technological innovation is cybersecurity.

Following the latest round of cybersecurity issues, stakeholders have responded by developing a mechanism to protect and minimise disruption to the confidentiality, integrity and availability of information. In the Indonesian context, this mechanism runs from the installation and hardware setup stage to monitoring processes and law enforcement. The following figure depicts the scope of cybersecurity in Indonesia.

Figure 3. Scope of cybersecurity

The scope of cybersecurity identified here raises the question of policy. There have been questions regarding whether the government will single-handedly be responsible for the whole scope of cybersecurity. What we understand is that policies – or the lack thereof – affects the dynamics of cybersecurity. Hence, this will also impact upon society.

After reviewing the existing regulations on cybersecurity in Indonesia, we noted that the legal foundation for cybersecurity is weak. Compared to other countries,

Indonesia lags behind in terms of ICT security policy and regulations. Malaysia, for instance, already has a Computer Crime Act, Digital Signature Act, Telemedicine Act (three of them have been enacted since 1997), Multimedia Act (1998), Payment System Act (2003) and a Personal Data Act (2010). Singapore has a set of similar regulations. Indonesia's lack of policies is a point on which all experts interviewed for this study agree, and one which Indonesian officials have also publicly acknowledged.

A deeper look into the history of cybersecurity policy in Indonesia shows that current policies revolve around the two main laws - the Telecommunication Law No. 36/1999 and the Information and Transaction Electronic Law (ITE) No. 11/2008 (DAKA 2013, Setiadi, Sucahyo, and Hasibuan 2012). The Telecommunication Law No. 36/1999 is a product of the Reformasi, and has contributed to the recent dynamics of the telecommunication sector in Indonesia. The Information and Transaction Electronic Law (known as ITE Law) No. 11/2008, on the other hand, is the first Indonesian cyberlaw (Kominfo 2015) - famous for the controversy around article No. 27 during various criminal defamation cases[1].

Both existing laws have their own limitations. The Telecommunication Law, while facilitating competition in the telecommunications industry, does not mention telecommunications infrastructure in the context of the internet. This makes it difficult to put certain cases into context. Additionally, while specific legislation on cybercrime has been enacted through the Law of The Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transaction (Articles 29-37), it has a limited scope, since it still requires other laws to supplement it. Due to these limitations, criminal cases related to cyber crimes are being punished with Criminal Procedural Law Codex (UU KUHAP), Consumer Protection Law No. 8/1999, Copyright Law No. 19/2002 or the Anti-Pornography Law No. 44/2008. But the Electronic Information and Transaction Law No. 11/2008 forms the cornerstone of cybersecurity related governance (as well as debates) in the country (see Figure 4).

Following the enactment of this law, Indonesia – like many of its South-East Asian neighbours – started to censor parts of the Internet. Under the administration of Tifatul Sembiring, the MCIT implemented Regulation No. 19 of 2014 on Controlling Internet Websites Containing Negative Content to promote "the safe and healthy use of the Internet" (Kominfo 2015). This is a sign of Indonesia's tight grip on the internet, as various reports claim[2] . Through this ministerial regulation, the Government provides a legal procedure to block 'negative websites,' with 'negative' being defined as containing pornographic or otherwise illegal material under the country's existing laws[3]. The reported 'negative' websites are later included in the 'TRUST+ Positive'[4] . According to the MCIT (2015), TRUST+ Positive has 763,126 websites in its blacklist, with most blacklisted for pornographic content.

The limitation of both laws has made regulators understand the importance of publishing technical regulations as supplements, especially for specific sectors. Technical regulations supplementing both laws have been sent from the MCIT to the Coordinating Ministry for Political, Legal and Security Affairs and even to the National Police. In the period of 2009-2015, more than 30 regulations and standards were issued to address cybersecurity issues, in particularly technical aspects (see appendix for details). However, most actors agreed that this new set of regulations is still insufficient, particularly with the complexity and growth of contemporary cyber threats. Regulations related to e-commerce, trademark/domain, privacy and security online, copyright, content regulation, dispute settlement and ICT critical infrastructure are among those needed. An expert shares the opinion on the lack of policies and its slow progress below:

> *PP 82/2012 actually instructs the release of dozens of Ministerial Regulations. However, according to my knowledge, only two or three are being released. So,*

1. The case of 'Prita vs. Omni Hospital' is the most infamous one of controversy following the article No. 27. The case was started in 2008, when Prita Mulyasari was falsely diagnosed at South Tangerang's Omni International Hospital. She wrote an email complaint to the hospital which then spread online in internet chat groups. This led to the hospital suing Prita for libel. See http://www.thejakartapost.com/news/2009/08/11/prita-takes-omni-case-supreme-court.html, accessed 28 September 2016.
2. Several cases Indonesia's tumultuous relationship with internet censorship include Netflix (2016), Vimeo, Imgur, Reddit (2014) and YouTube (back in 2008). The Citizen Lab of Toronto, Canada and Elsam of Jakarta, Indonesia are two one of the institutions providing report on Internet censorship and surveillance in Indonesia since 2010. Several media also provide the data on this issue. See http://www.rappler.com/world/regions/asia-pacific/indonesia/bahasa/englishedition/120513-netflix-censorship, accessed 27 July 2016
3. In November 2014, the regulation was challenged by a group of CSOs and brought to the Supreme Court for judicial review. However, the Supreme Court upheld the regulation without a legislative review.
4. A database system promoted by the MCIT contains list of websites with allegedly negative content. See http://www.makarim.com/index.php/site/detailNews/id/306/cat/8/thn/2014/bln/October/title/INTERNET%20CONTENT%20CENSORSHIP%20STRENGTHENED, accessed 28 July 2016..

there are ten more regulations which should be released from the MCIT, including policies on digital signatures or electronic certificates, among others - also for e-commerce. The path is still long and tough for Indonesia. (Undisclosed, Academia, Interview, July 2016)

Realising that effective cybersecurity governance is about regulation, awareness and coordination together, the government responded by initiating the establishment of a National Cybersecurity Agency (BCN - Badan Cyber Nasional) while working to fix the regulation and raise national awareness at the same time. But the road to establishing the agency seems to be bumpy. And with several agencies and ministries eagerly promoting themselves as the coordinator, this reactive behaviour from the government illustrates the overlapping governance of cybersecurity.

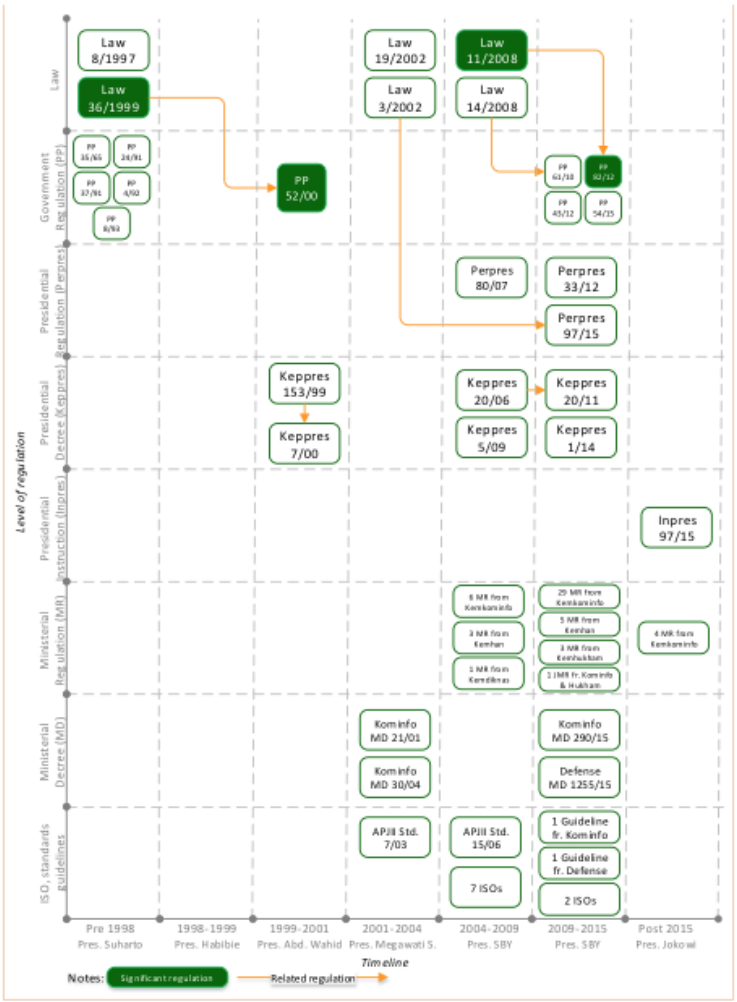


Figure 4. Cybersecurity-related regulations and standards

While weak in legislative terms, Indonesia is quite strong on technical and procedural measures. International cooperation is also not deemed to be a problem since Indonesia is enhancing its international cooperation with various organisations, security experts and forums in order to improve its understanding of global threats[5]. As an embodiment of this principle in cybersecurity, Indonesia has became a full member of APCERT and FIRST and a founder of the OIC-CERT.

As for technical measures, Indonesia has officially recognised compliance requirements through SNI/ISO/EIC 27001: 2013 concerning Information

5. This spirit is in line with the political stance stated in the constitution, "to participate toward the establishment of a world order based on freedom".

Security Management Systems. To raise security awareness and to track progress, Indonesia has its own framework for assessing domestic information security across government agencies. The KAMI index (the National Information Security Index) evaluates five areas of information security: governance, risk management, framework, asset management, and technology[6]. However, there is still a lot of work required. The absence of an officially recognised national governance roadmap for cybersecurity is one urgent priority (ITU 2015). With regards to the implementation of international standards, the ITU (2015) noted that Indonesia has not yet officially approved national (and sector specific) cybersecurity frameworks. This is also the case for certification. Currently, Indonesia does not have any officially approved national (and sector specific) cybersecurity frameworks for the certification and accreditation of national agencies and public sector professionals. The Association of Indonesia Internet Providers (APJII) confirmed these findings by adding that currently the existing standards are mostly adopted from regional or international entities (interview, 2016).

Without adequate technical capabilities to detect and respond to cyber attacks, states and their respective entitities remain vulnerable. All stakeholders, in particular the government, therefore need to be capable of developing strategies and the required skills to deal with cyber incidents at a national level. Such strategies and required skills need to be incorporated into national policies on cybersecurity.

The role of non-governmental stakeholders

In terms of BCN's establishment, non-governmental stakeholders such as the business sector (APJII and Nawala) and CSO's (ICT Watch, Elsam, among others) were invited to the discussions. However, it is still difficult for non-governmental actors to get more involved in the process. Most of the time, interpersonal relationships matter more than organisational engagement, as stated by our respondent:

"... My friends from the business sector are facing difficulties getting involved in the discussion [of cybersecurity]... they might be invited for a meeting once or twice, but here in Indonesia, what matters more is interpersonal relations [between non-government actors and the government]... So we [non-government actors] need to check whether we have the same voice towards the government [during the discussion on BCN]. Often there are people who use their personal interest to get close to the government, and they cannot represent our [non-government actors] voice." (Undisclosed, Private Sector, Interview, July 2016)

From the statement above, it seems that the non-government actors are also fragmented when it comes to cybersecurity coordination - for example, even the idea of having a cybersecurity coordinator divides the private sector and CSOs. Often, the government will invite those who agree or have the same voice in order to make discussions easier.

The institutions that seem to be the most active in inviting other stakeholders from CSOs, the private sector and academia are the MCIT and the National Resilience Council (Dewan Ketahanan Nasional). The National Encryption Agency has also invited CSOs to cybersecurity discussions, but not as often as the former two agencies. Unfortunately, the Coordinating Political, Legal and Security Affairs Ministry (Kemenkopolhukam), as the initiator of BCN, seems to be less active in engaging with non-government actors. The reason being is Menkopolhukam's perception of cybersecurity as relating to issues of sovereignty – which means their approach is more militaristic.

"... It [the approach] should be varied [not only militaristic]... But they [Kemenkopolhukam] said that this [cybersecurity governance] is for the great

6. The KAMI Index begins with a self-assessment, followed by an evaluation of the answers and a interview by assessors. The 2012 internal findings reveal that the highest scores were in the technology and asset management areas while the greatest weaknesses, were in risk management and governance

sake of nation, so citizens should believe in them, they [Kemenkopolhukam] will handle it [cybersecurity governance]. Those statements are our [the CSOs] biggest concern." (Undisclosed, Civil Society, Interview, July 2016)

Non-government actors are still working in their own separate areas. The private sector has established the necessary infrastructure and network protection, while CSOs push for a more 'humane' approach to cybersecurity by advocating for the inclusion of human rights and freedom of expression values in regulation. Both actors are doing what is within their reach with regards to cybersecurity governance, without the presence of government.

However, all of our non-government respondents agree that there is no need to establish a new coordination agency, such as BCN, which could gather the scattered operational expertise on cybersecurity.

"If the agency is working on its own, there is no need [to establish BCN], because it [the agency] has to cooperate with all aspects and all actors that already have their own expertise. Which actor should be approached when there is an attack [for example]? what step should be taken to handle a national attack [for example]… [The agency should be capable to] cooperate with different actors, knowing what resources and infrastructure each actor has, and which actors should be approached [in case of a cybersecurity violation]." (Undisclosed, Private Sector, Interview, August 2016).

It is evident that the process of establishing the BCN cannot be completely independent from politics. This means that advocacy to coordinate national cybersecurity will fall short. Until this report is written, even the business sector and CSOs have not performed a coordinated advocacy campaign towards the government. The reason is that the government is still unsure about its plan for the BCN and is therefore offering only a vague opportunity for non-government actors to get involved. Recommendations on how better advocacy strategies could be implemented will be outlined in the next chapter along with synthesis and lessons learned.

04

SYNTHESIS AND RECOMMENDATION

There are many challenges in discussing cybersecurity in Indonesia, which are highlighted on the below diagram.

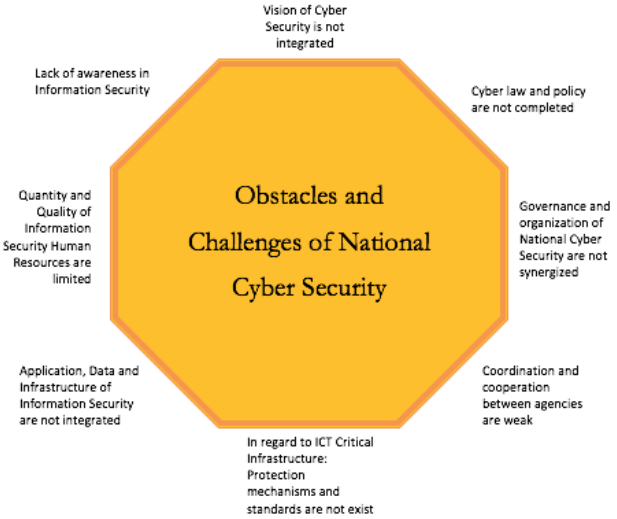


Figure 5. Obstacles and Challenges of National Cybersecurity
Source: Adapted from Detiknas (2013)

These obstacles and challenges cover several aspects which need to be addressed to effectively manage cybersecurity governance. Our study identifies three key gaps:

1. Different understandings and approaches towards cybersecurity

The controversy surrounding cybersecurity governance starts with its definition. It is not merely linguistic pedantry. The way the cybersecurity is defined and understood reflects different perspectives and approaches, as well as policy interests (Kurbalija 2014). As interpreted from our findings, technical communities see cybersecurity governance through a technical, infrastructural lens, and tend to focus on the development of different standards and applications.

By contrast, civil society organisations, in particular human rights activists,

view it mainly from the perspective of freedom of expression and privacy. Law enforcers and intelligence agencies tend to focus on issues that resonate with the protection of national interests.

Realising that the internet is not just another new technology – since it has an important role as an enabler for development – a new approach should be embodied in how it is governed. This new approach to this new technology should not limit the discussion over its governance by focusing on a single perspective. Rather, cybersecurity governance should embrace various perspectives – technical, legal, social, economic and developmental – and also enable all stakeholders to take part. This approach also reflects the true nature of the internet – which is inclusive by birth, developed by both the public and private sectors, academia and civil society, and operates across borders. The internet is fundamentally participatory and bottom-up, a heterogenous but robust ecosystem.

In Indonesia, a participatory approach which reflects these values has yet to be realised. While some early efforts at engagement have been made, decisionmaking remains exclusive to the government, leaving other stakeholders voiceless in the process. This is also the case for cybersecurity governance. While the government is aware that effective cybersecurity is about regulation, awareness and coordination, the topic is still relatively new and not a priority. This is the basic challenge of Indonesia cybersecurity.

2. Human resources capacity

The digital divide and lack of human resources in the area of information security are also issues add an additional layer of complexity. Eager to improve the capacity of human resources in the area, MCIT has developed a standard framework of competence in information security, in cooperation with the private sector and academia.

The standard, known as SKKNI Sector of Information Security, is used to set the baseline of technical skills for those who perform information security functions in organisations whose area is the implementation of information security (Decree of the Minister of Manpower No. 55/2015). In line with this standard, the Directorate of Information Security of MCIT regularly conducts technical assistance and awareness raising programs to promote cybersecurity courses in higher education and for the general public, as well as providing professional training programs (Kominfo 2015).

According to the ITU (2015), Indonesia currently has approximately 500 public sector professionals certified under internationally recognised certification programs in cybersecurity such as ISO270001, CEH, CISA, CISM and CISSP. The number, however, is not sufficient for Indonesia. As representatives from APJII (interview, 2016) added, human resources in cybersecurity are dominated by foreign workers since local expertise is still very low.

3. Coordination

Complex problems require multidimensional approaches. Therefore, in order to improve cybersecurity governance, the implementation of the multistakeholderism principle is highly important. Without mutual cooperation and collaboration among stakeholders (from public service entities to the private sector, academia and civil society) problem solving in cybersecurity-related issues will be one-dimensional and incomplete. An inclusive mechanism should certify the decisions and be reflective and responsive to both national concerns and affected populations. Recalling the importance of the cybercrime principle, it is imperative to

provide a coordinating agency (either by promoting one of the existing units or creating a new body) which is responsible for coordinating efforts when needed – with full support from all parties involved. The coordinating agency should consist of individuals who have integrity and are highly competent.

At the operational level, each sector needs to have their own emergency response team to handle incidents within their sector, each with clear roles and responsibilities. This action should be directed within a set of proper regulations and roadmaps without forgetting the importance of building national awareness. To conclude, a trio of 'regulation, awareness and coordination' should be the mantra in national cybersecurity governance.

Underpinning issues

Cybersecurity is often mentioned as one of the preconditions for the rapid growth of e-commerce. Without secure and reliable access to the internet, customers will be reluctant to provide confidential information online. Therefore, it is unsurprising that the business sector in Indonesia is leading the push for faster developments in cybersecurity; more so than the government. However, since the 2013 Snowden revelations, the government has started considering mitigation tactics, including encouraging internet companies to store citizens' personal data on data centres within local jurisdictions. The same circumstance also accelerates political tension on the issue.

Our study found that the focus of cybersecurity in Indonesia is on defence, war and sovereignty. One of the facts that speaks for this claim is the recent heated debate over the establishment of BCN (Badan Cyber Nasional – National Cybersecurity Agency). The BCN's perspective on cybersecurity focuses on the protection of critical infrastructure such as public airports and electricity grids. Rudiantara, the Minister of Communication and Informatics, has on various occasions emphasised the need for an organisation whose remit is the full protection of Indonesia from cyber threats – from the identification stage through to the recovery process.

While the main task is to prevent cyber attacks, this agency would also be responsible for developing a strategy to strengthen Indonesia's defence against cyber threats and attackers. In accordance with the strategy, the agency would also work to increase public awareness about the cybersecurity landscape. Recent developments indicate that the government has decided to cancel the plan to set up a national cyber agency due to budgetary constraints and a moratorium in establishing new agencies[1] . It remains to be seen how the discourse, as well as the publication of legal documents regarding the agency, will evolve in the near future.

In line with this idea of a coordinating agency, MCIT also plans to launch a cybersecurity roadmap, which would intend to provide Indonesia with a national cybersecurity benchmark for the non-military sector. According to Rudiantara, MCIT, together with other regulators and specific sectoral operators, has developed a plan for mandatory business processes for three sectors; finance and banking, transportation, and energy[2]. In accordance with this plan, the Ministry of Administrative and Bureaucratic Reform will assist businesses with these processes. While it seems to be a solid process, several questions, in particular related to the coordinating agency, remain. What kind of agency will take charge? Who will be responsible for leading this – the Minister, the Coordinating Minister, or ministerial level officials? How will the reporting mechanism work and what will be the structure of this agency – will it report directly to the President?

The roadmap is apparently part of the upcoming presidential regulation

1. This is the popular belief among cybersecurity actors since some media coverages stated that the government diverts the task to an existing agency, in this case is the National Encryption Agency. For example, see http://tekno.kompas.com/read/2016/06/22/14494137/badan.cyber.nasional.batal.dibentuk, accessed 18 July 2016. However, when the author asked the question to the National Encryption Agency, the Agency responded that until there is a legal regulation (in this case is a Presidential Regulation) on the coordinator issue, the option will be remain open.
2. As stated by Mr. Rudiantara, Minister of Communication and Informatics via online forum discussion on 13 July 2016. In addition, the document on three sectors will be available for general public at the end of 2016 (Representative of MCIT, Interview, October 2016).

(Perpres) encompassing e-commerce, which would also be the part of the 14th economic policy package. According to several media reports, the Perpres would focus on seven issues including taxation, cybersecurity and communications infrastructure[3]. The government, however, has declined to confirm when the new policy package would be issued. Regarding this discourse, civil society and academic communities argue that the policymaking process concerning the roadmap and coordinating agency should embrace the multistakeholder approach.

Aside from this coordination issue, it will be interesting to see whether the human rights perspective is integrated into the policymaking process. The protection of human rights (privacy, freedom of expression, internet access), in this case, is highly relevant for the policymaking process in cybersecurity. This is not only a value-based priority, but also a practical tool for ensuring that the internet remains open and secure. Protecting access to individual devices is actually indirectly preventing institutions or companies datasets from violation, which is conducted through end users' backdoors. Concerns of the end users, however, are usually not about possible greater damage (often due to ignorance) as a result of the violation, but rather about privacy and rights in general.

Recommendations

Having presented the findings and our conclusion, we envisage at least three immediate action points in cybersecurity governance:

First, the need to set priorities through a holistic approach

A holistic approach should facilitate not only the technical but also the legal, social, economic, and developmental aspects of digital development. While maintaining a holistic approach to the negotiations, each actor, from government officials and business representatives to academia, think-tanks and civil society organisations, should identify their key priority issues. This kind of approach to the cybersecurity governance agenda should help all actors to focus on a particular set of issues. This should lead towards more substantive and possibly less politicised negotiations.

According to one of our respondents, the sets of regulations that are currently being used to refer on cybersecurity[4] still does not incorporate human rights principles. Therefore, one of CSOs' priorities must be to have these human rights principles included in the Bill. The private sector, such as APJII, could focus on infrastructure-related governance issues, while academia focuses on the social and economic dimensions of cybersecurity, and technical communities the issues related to network security.

However, the actors involved are still working in silos and there is a lack of coordination with one another. The reason is generally that they do not feel any need to communicate with each other as long as they can handle what is in their domain. The other reason is that there are only a few actors who understand cybersecurity, and still fewer who understand how it interacts with human rights. Achieving the holistic approach needed for cybersecurity governance will be a long journey, not only at the national level but also at the regional and international level.

Second, strengthen the multistakeholder approach.

Cybersecurity policymaking in Indonesia has already implemented the multistakeholder approach, with the government inviting the private sector, civil society organisations, and academia to cybersecurity discussions. However, most of the time private sector and civil society organisations

3. See http://www.thejakartapost.com/news/2016/09/28/incentives-sought-to-propel-e-commerce-.html, last accessed 28 September 2016. Also see http://bisnis.news.viva.co.id/news/read/827475-paket-ekonomi-jilid-xiv-pemerintah-bakal-atur-e-commerce, last accessed 28 September 2016.
4. Currently, there are several regulations that are being utilised to refer on cybersecurity in Indonesia, among others: Law No. 11/2008 on Electronic Information and Transaction, Law No. 36/1999 on Telecommunication, Law No. 14/2008 on Public Information Transparency and Government Regulation No. 82/2012 on Implementation of Electronic System and Transaction. See http://aptika.kominfo.go.id/index.php/artikel/138-peta-masa-depan-keamanan-siber-indonesia, last accessed 29 November 2016.

are only allowed to participate in a more passive way, by listening to the government, without much opportunity to criticise governments policies and actions. In order for the multistakeholder approach to function well, all stakeholders need to have similar opportunities to voice their concerns. In the latest round ofdiscussions, the idea that the National Encryption Agency (NEA) could potentially become the leading actor in cybersecurity was rasied. Therefore, it is important for civil society to actively engage with the agency. This report identifies two means by which CSOs could engage with the government, including the NEA.

Firstly, CSOs could participate actively in cybersecurity discussions. For the last year, the NEA held several discussions on cybersecurity which involved civil society organisations. Aside from the differences in understanding and approach towards cybersecurity, the discussion has become one prominent means for CSOs to engage with the NEA and to assist the government in composing policies related to cybersecurity. CSOs are also urged to invite government agencies and other fellow civil society to various CSO forums on cybersecurity. This could increase CSOs' visibility on the issue, while also increasing the awareness within civil society of cybersecurity.

Secondly, CSOs could present policy briefs or factsheets on cybersecurity issues - on human rights principles in cybersecurity governance - from the citizens' point of view. Several CSOs, such as ICT Watch and Elsam, are regularly updating their knowledge on cybersecurity, and have even published desk research and factsheets. These documents are rarely shared with the government, even though they are accessible for public use. CSOs could utilise the discussions held by government agencies to present factsheets and policy briefs, especially on human rights principles in cybersecurity governance. Since CSOs in Indonesia also engage quite closely with the private sector, it seems plausible that they could construct a joint policy brief or factsheet that can be presented to the government, which would mean the government was regularly updated on recent issues concerning cybersecurity from the citizens' and private sector's point of view.

These two methods could be performed to establish a coordination mechanism that accommodates each actor's principles. Furthermore, it could establish a solid understanding that cybersecurity is not merely related to defense and cyber war but also to network security, critical infrastructure, and business transaction security, among others things. Prior to strengthening the multistakeholder approach, it is of course imperative that the government also manages its inter-institutional coordination.

Third, enhancing awareness and improving capacities.

We have outlined how cybersecurity awareness in Indonesia is still low and that there is an urgent need to increase this awareness, not only within civil society but also for government officials. Cybersecurity can still seem a big word, especially in civil society. Therefore, to enhance awareness, one should start by improving people's basic understanding of issues such as personal data privacy.

Other weaknesses Indonesia should address are related to human resources. Here, there is an educational deficit. The challenge for the government is how to raise people's awareness of cybersecurity[5]. At the same time, the government must also build its own internal capacity. Fortunately, officials seem to share the same perspective. The Minister of Communication and Informatics has emphasised that the most urgent issue to be addressed with regards to cybersecurity is awareness building and removing sectoral egos.[6]

5. According to Wahyudi Djafar from Elsam, Indonesia has a serious problem in addressing data privacy for at least three following aspects: (i) due to regulation problems; (ii) escalation of threats; and (iii) people have a very low awareness to protect their own privacy. See http://elsam.or.id/2015/01/perlindungan-hak-atas-privasi-tantangan-berat-butuh-sinergi-dari-semua-pemangku-kepentingan/, accessed 22 July 2016. See also http://tekno.liputan6.com/read/2491777/indonesia-harus-punya-regulasi-perlindungan-data-pribadi, accessed 22 July 2016.

6. http://tekno.kompas.com/read/2015/08/24/13375717/Oktober.Indonesia.Punya.Blueprint-Pertahanan.Cyber?utm_source=RD&utm_medium=box&utm_campaign=Kaitrdread/2015/08/24/13375717/Oktober.Indonesia.Punya.Blueprint-Pertahanan.Cyber?utm_source=RD&utm_medium=box&utm_campaign=Kaitrd

Success stories and lessons learned

There are two notable success stories and lessons learned for CSOs with regards to cybersecurity in Indonesia. Firstly, CSOs have been successful in opening up discussions between the government and other actors, including the private sector. This success started from the initiation of ID-IGF, an Indonesian version of Internet Governance Forum.

At the time, several CSOs representatives had begun discussing internet issues with the private sector and government, particularly the MCIT. The ID-IGF in Indonesia in 2013 was structured around a multistakeholder approach and was a success. After the ID-IGF, the discussion between these actors moved forward; not merely on internet governance, but also on net neutrality and cybersecurity, among other things. These activities have flourished into comprehensive engagement between government, CSOs, the private sector, technical communities, and academia. The ID-IGF has become an important hub in which internet-related discussions take place and the multistakeholder approach is implemented.

Secondly, CSOs have managed to start increasing citizens' awareness of cybersecurity by means of informal discussions, fact sheets and desk research. Although it is still at the incipient stage, these activities help to spread awareness of cybersecurity issues, particularly those in the citizens' interest such as privacy and human rights.

With the success stories of CSOs engaging with other actors, it is plausible that CSOs could become a focal point for discussions on cybersecurity, including the debate about how the coordination agency should be established.

Moving forward: What more could be done?

To conclude, there are three important things that could be done by CSOs in terms of cybersecurity advocacy in Indonesia:

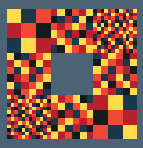
1. Increase awareness. Although this applies to all stakeholders, CSOs who actively engage in cybersecurity forums and discussions – both at the regional and international level – could take the lead in disseminating knowledge and concerns, at least among civil society, through regular factsheet updates, trainings and workshops.

2. Capacity building. This is needed not only on the issue of cybersecurity and human rights, but also on negotiation skills, as CSOs should be prepared to engage with the bureaucracy and government officials. Furthermore, a comprehensive knowledge of government regulation should be fostered among CSOs. For this to happen, regular training at both the regional and international level is needed. CSOs could then bring the national case to be discussed with other CSOs from around the world and learn lessons from other partners. At the national level, forums such as FDD (Forum Demokrasi Digital – Digital Democracy Forum) and TEDI (Temu Digital – Digital Meet Up) could become important channels and platforms from which to disseminate knowledge.

3. Increase and maintain visibility. In order to be involved in cybersecurity discussions at the national level, CSOs should be persistent in maintaining their commitment to advocacy on this issue. With this proactive approach, the government will become aware of CSOs' presence and concerns. This visibility will help the government in identifying CSOs when they begin to involve stakeholders in cybersecurity discussions.

All of the above strategies could be implemented through cybercrime

engagement, and includes both cybersecurity and human rights discussions. It is clear that the recommendations and success stories above could not be performed only by one or two actors,. They would need to be performed in coordination between actors. For example, the private sector could provide trainings and workshops for government officials to improve the officials' knowledge of cybersecurity; technical communities could provide workshops on recent technological developments; and civil society organisations could help the government formulate policies and disseminate information related to cybersecurity to citizens.



GLOBAL PARTNERS DIGITAL

Human rights in a connected world

GLOBAL PARTNERS DIGITAL
Second Home
68 - 80 Hanbury Street
London E1 5JL
+44 (0)20 3 818 3258
gp-digital.org