Meeting the cyber security challenge in Indonesia

An analysis of threats and responses

A report from DAKA advisory

Commissioned by

British Embassy
Jakarta

Contents

Cover photo: © iStockphoto.com/loops7

Foreword

His Excellency Mark Canning, British Ambassador to Indonesia.

I have been fortunate to have had two tours of duty in Jakarta and I often reflect on how different they have been in terms of technology.

When I left Indonesia in 1997, contact with friends and family, was done by letters or expensive telephone calls. Email was in its infancy. There were no PCs in the British Embassy.

Just a few years on, it's impossible to imagine our daily life without the internet and the opportunities it offers for immediate connection with anyone, anywhere, at any time. In both the UK and Indonesia the internet is transforming the way we do business and communicate. In Indonesia, there are over 55 million internet users (many of whom are part of the Facebook and Twitter community) and nearly 50% of Jakarta's population owns a smart phone. We have quickly become dependent on the social benefits that the internet has brought us - reading the news as it happens, keeping in touch with friends and family, shopping, booking flights and checking in 'virtually' at the airport. Whilst the internet has the capability to continue driving economic growth, it also offers the potential for threats and fraud that could not have been imagined twenty years ago.

Cyber crime is a very real threat, and its prevention is one of the UK's top security priorities. The threats posed by cyber crime need to be understood and urgently tackled. We have seen what happens when it goes wrong – websites defaced, citizens defrauded and critical infrastructure targeted. But the nature of cyber security means we can't tackle it alone; and the response should not just consist of state involvement, but a variety of interested partners, from industry, civil society as well as internet experts coming together in a process known as the 'multi-stakeholder approach'.

The UK's 2010 National Security Strategy rated cyber attacks as a top threat and set £650 million aside over four years to develop our response. The UK's Cyber Security Strategy (available online) was published in November 2011 and determines how we will tackle these threats yet ensure a balance of security with respect for privacy and fundamental rights. At the heart of our cyber security agenda is the belief that cyberspace should remain an open space which allows the free flow of ideas, information and expression. The UK has taken a lead in establishing international discussions on cyber security, bringing together Ministers, senior government officials, industry leaders and representatives of the internet technical community and civil society from 60 countries for the inaugural Cyber Conference in London in late 2011. This was followed by the Budapest Cyber Conference in 2012, and we are looking forward to Seoul hosting the third Cyber Conference later this year.

I am delighted that the British Embassy Jakarta has been able to fund this report on cyber security. Its analysis and recommendations will help identify the threats facing Indonesia and highlight possible solutions. I am sure that this report will provide Indonesia and the UK with more opportunities to work together on cyber security, for the security and prosperity of the citizens of both our countries.

About the project

Meeting the cyber security challenge in Indonesia: An analysis of threats and responses is a report from DAKA advisory written by Kim Andreasson. It was commissioned by the British Embassy in Jakarta on behalf of the British Foreign & Commonwealth Office. The report does not necessarily reflect the views of the sponsor.

The aim of the report is to raise awareness of cyber security and the potential consequences of cyber threats on Indonesia, as well as to provide suggestions on which to build preventative and reactive policy measures. Although the report does not use a consulting framework per se, a SWOT (strengths, weaknesses, opportunities, threats) approach was used in deriving the recommendations.

To uncover cyber security threats and responses in Indonesia, and those that affect it from a global perspective, DAKA advisory conducted extensive desk research and interviews with a mix of international and local experts. We would like to thank the following people and organisations for their contributions (listed alphabetically by surname):

- Ian Brown, Associate Director, Cyber Security Centre, University of Oxford, United Kingdom
- Mohammad Guntur, Senior Vice President, IT Strategy, Architecture & Planning Group, Bank Mandiri, Indonesia
- Bambang Heru, Director, Directorate of Information Security, Indonesia
- Benjamin Keller, Vice President, Service Operations, XL, Indonesia
- Benedicta Kristanti, Officer for Counter-Terrorism, Ministry of Foreign Affairs, Indonesia
- Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda
- Rudi Lumanto, Chairman, Indonesia Security Incident Response Team on Internet Infrastructure, Indonesia
- IGN Mantra, Chairman, Indonesia Academic CERT/CSIRT, Indonesia
- Simon Mui, Head of Subsidiaries and Acquisitions, Group Information Security, Standard Chartered Bank, Singapore
- Yudhistira Nugraha, Head of Information Security Risk Management, Directorate of Information Security, Indonesia
- Marco Obiso, Cybersecurity Coordinator, International Telecommunication Union
- Jaziar Radianti, Post-Doctoral Researcher, Centre for Integrated Emergency Management, University of Agder, Norway
- Budi Rahardjo, Head of Indonesia Computer Emergency Response Team, Indonesia
- Yudho Giri Sucahyo, Professor, Faculty of Computer Science, University of Indonesia, Indonesia
- Daniel TS Simanjuntak, Deputy Director for WMD and Conventional Weapons, Ministry of Foreign Affairs, Indonesia
- Winston Tommy Watuliu, Police Colonel and Head of IT & Cyber Crime Section, Indonesian Police, Indonesia

Executive summary

Governments, businesses and civil society around the world are increasingly seizing the opportunities associated with information and communications technologies (ICTs) to gain a competitive position or improve on their socio-economic situation, often both.

ICTs are an integral part of a modern society and several international studies show their importance to all aspects of development. Global leaders, such as Sweden, illustrate the potential of going digital by embracing ICTs and the educational means to capture their benefits. But an increase in cyber dependency also means an increase in risk.

As global and domestic economies, as well as individual businesses and civil society at large, increasingly look to ICTs to improve their well-being, it also means that cyber threats can affect all aspects of society, including the free and accurate flow of information, trust, and socio-economics. Digital development marches on, and those that cannot adapt their strategies to encompass cyber security are increasingly vulnerable to a growing number of cyber threats. In order to meet them, there is a role for all stakeholders: from the educational system and user awareness to government regulation to industry interest.

As a rapidly emerging market, Indonesia has widely embraced ICTs. It also outpaces many countries at the same level of development in several areas. For example, its recognition of using ICTs to improve future growth prospects has led to its highly competitive telecommunications market. In turn, this stimulated a rapid uptake of mobile devices and social media usage among the population, from which the country now has a broader base to further leverage ICTs. Indonesia stands to benefit greatly from this development at the national level, including a further supply of services and the demand for them.

To uncover cyber security threats and responses in Indonesia, and those that affect it from a global perspective, this report is based on a combination of extensive desk research and interviews with a mix of international and local experts. Parts 1 and 2 introduce cyber opportunities and threats as well as their potential implications around the world, including in Indonesia specifically.

To better understand the current cyber security situation in Indonesia, parts 3 through 5 provide an overview of current initiatives and key stakeholders in the country before evaluating its current weaknesses and proposing steps in order to meet the cyber security challenge and seize the full socio-economic potential of a digital society.

The key findings are as follows:

Opportunities: There is a strong link between the adoption of ICTs and socio-economic development, and it is global in nature. This has led to both rising availability of ICTs as well as usage of them. The combined increase in adoption and supply and demand is increasing our cyber dependency.

Threats: Higher cyber dependency naturally leads to an increase in risk and there are a wide variety of threats to governments, businesses and civil society alike. Given its current level of development, Indonesia is particularly vulnerable to certain types of cyber threats, primarily non-political cyber crimes. Although they may not constitute physical danger, cyber crime can be costly, as a number of international estimates suggest. Based on those sources, this report also finds the potential financial implications for Indonesia to be high.

Responses: By classifying cyber threats as either politically motivated or non-political in nature, it appears that almost all cross-national agreements focus on cyber crimes rather than cyber security more broadly. Coincidentally, the current response environment within Indonesia also emphasises cyber crime, despite growing calls for cyber security measures.

Ways forward: As Indonesia continues to develop rapidly and increase its cyber dependency in the process, the country will become more vulnerable to a growing number of sophisticated threats, some of which may be politically motivated. As a result, Indonesia must put cyber security into a wider societal context and make necessary preparations to meet this challenge.

Strengths and weaknesses: When assessing Indonesia’s current environment for cyber security preparedness, strengths include recognition of its importance, indicated by the many initiatives in place. The weakest areas are the regulatory framework, capacity building in terms of awareness, and a lack of coordination among the multiple agencies involved in cyber security, which is in part due to the lack of a formal strategy.

Recommendations: Based on the key findings, this report concludes with six suggested steps towards achieving greater cyber security in Indonesia:

1. Make cyber security a priority, at home and abroad
2. Assess what needs to be done
3. Strengthen the regulatory environment
4. Enhance awareness and improve skills
5. Coordinate a stronger multi-stakeholder approach
6. What gets measured gets done: develop a cyber security strategy

1 Introduction

The rise of the information society has been swift and is global in nature. The international dimensions of cyber security, therefore, cannot be ignored as they affect everyone who is connected to the network. This report begins with an assessment of global trends followed by an evaluation of their applicability to Indonesia.

The rise in cyber dependence

A basic framework to gauge levels of cyber dependence across the world or in individual countries includes an assessment of three distinct areas: competitiveness and the link between ICTs and socio-economic factors; supply-side initiatives, such as the organisational move towards ICT; and, demand-side factors in terms of connectivity and usage.[1]

Competitiveness and the rise of the Internet

Today, ICTs contribute strongly to economic growth and better social outcomes around the world (see box on page 9 for examples). Global and domestic economies, therefore, must recognise the tie between competitiveness and the Internet, including in their education and user engagement initiatives, while ensuring resilience of computer networks.

“ICTs are at the core of our economies and societies and we need to be able to trust them so we can reap all the benefits they offer,” says Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda. This is important to the public and private sectors as well as civil society. By 2015, 90% of all jobs in the Europe are reckoned to require digital literacy.[2]

[1] Adapted from Kim Andreasson, editor, Cybersecurity: Public Sector Threats and Responses: http://www.crcpress.com/product/isbn/9781439846636

[2] European Commission, Digital Agenda: http://ec.europa.eu/europe2020/pdf/themes/digital_agenda_ict.pdf

Opportunities trump threats: Potential economic benefits from the Internet

The opportunities associated with going digital are vast and there is mounting evidence around the world of their potential economic benefits. Recent examples include:

- According to the McKinsey Global Institute, a consultancy research arm, the Internet contributed an average of 3.4% to GDP in 2011 across the G8 countries plus South Korea, Sweden, Brazil, China and India. Although the range varied from Russia (0.8%) to Sweden (6.3%), it illustrates the impact across the world, as well as the potential opportunities if emerging markets can catch up.[3]
- Because of a combination of cost savings and productivity gains, some governments are striving to be "digital by default," meaning that services are primarily delivered through digital channels. In the United Kingdom, PwC, an accounting firm, reckons that if the entire population were online, the total economic benefit to the country would be at least GBP 22bn.[4] In Denmark, the government estimates it will save EUR 160m a year once public service communication is completely digital, which it is mandated to be by 2015.[5]
- The economic benefits are global in nature and also appear to rise as technologies evolve. A commonly cited example is the World Bank's 2009 report on Information and Communication for Development, which found that every 10% increase in broadband penetration can increase economic growth by 1.38% in low- and middle-income countries.[6]

Demand: Connectivity and the rise in usage

Whether it is online banking or electronic delivery of public mandates (e-government), people are jumping at the opportunity to receive information and conduct services on the Internet. The rapid rise in consumer and constituent demand is driven by underlying factors, such as a decreasing cost of access and the increasing availability of mobile solutions through which to conduct digital communication. The International Telecommunication Union (ITU) ICT price basket, a measure of affordability, shows an 18% decrease in the price of access globally compared with the previous year with particularly declining rates in developing countries.

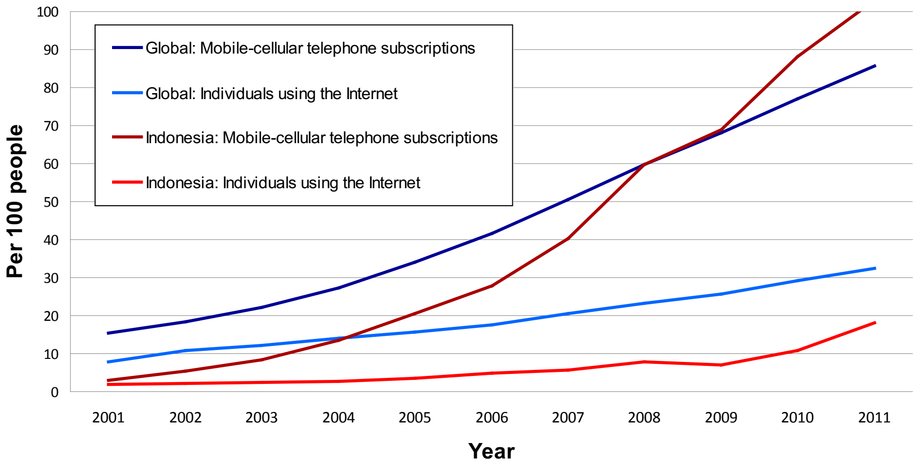
[3] McKinsey Global Institute, Internet matters: http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Internet_matters

[4] PwC, Champion for Digital Inclusion: The Economic Case for Digital Inclusion: http://www.parliamentandinternet.org.uk/uploads/Final_report.pdf

[5] Danish Agency for Digitisation, eGovernment strategy 2011 – 2015: http://www.digst.dk/Home/Digitaliseringsstrategi/Download%20strategien

[6] World Bank, Information and Communications for Development 2009: http://siteresources.worldbank.org/EXTIC4D/Resources/IC4D_Broadband_35_50.pdf

Figure 1: Growth in Internet and mobile usage in Indonesia and the world



Source: ITU World Telecommunication / ICT Indicators database.

Supply: The move towards ICTs

To meet demand and improve productivity, businesses and governments are moving their processes online, hence also increasing their dependency on fixed and mobile networks. The greater use of ICTs is tracked globally by a number of reports, including the annual Global Information Technology Reports from the World Economic Forum (WEF).[7] In 2012, Sweden led the world in its Networked Readiness Index, which “measures the extent to which 142 economies take advantage of ICT and other new technologies to increase their growth and well-being.” Indonesia was in 80th place. The primary source for tracking government supply-side efforts is the biennial E-Government Development Index in the United Nations (UN) E-Government Survey, which in 2012 found that “[p]rogress in online service delivery continues in most countries around the world,” with the Republic of Korea leading the way and Indonesia ranking 97 out of 193 UN member states.[8]

The view from Indonesia

The global framework can also be used to illuminate the role of ICTs in Indonesia’s competitiveness as well as the supply-side and demand-side factors in the country. This exercise finds an increasing importance of ICTs to Indonesia’s economy and the country’s recognition thereof. Compared to other countries around the world, Indonesia is currently rated as average in both supply and demand for ICTs, although it is rising rapidly in both areas.

[7] World Economic Forum, Global Information Technology Report: http://www.weforum.org/issues/global-information-technology

[8] United Nations, E-Government Survey: http://unpan3.un.org/egovkb/

Country data for Indonesia

Population: About 248m
Capital: Jakarta, with about 9m people

GDP per capita (PPP): About USD 5,000
GDP growth: About 6% in 2012

URL for the e-government portal: www.indonesia.go.id
WEF Networked Readiness Index ranking: 80 (out of 142 economies)
UN E-Government Survey ranking: 97 (out of 193 member states)

Number of mobile phones: About 250m
Number of Internet users in 2012: About 63m
Number of Internet users in 2015: Estimated at 139m

Sources: CIA World Factbook; Indonesian Internet Service Provider Association; UN; WEF

Indonesian ICT competitiveness

Indonesia recognised ICTs as an industry of the future in the Presidential Regulation No.28 Year 2008 on National Industrial Policy. Further, the nation's Masterplan for Acceleration and Expansion of Indonesia Economic Development 2011-2025, commonly referred to as MP3EI, states: "Development of ICT should continue to be accelerated in order to improve the nation's competitiveness to create knowledge based economy."[9] Explicitly recognising the findings of the World Bank study, Indonesia is also aiming for the creation of a National Broadband Network (NBN) by 2015, according to MP3EI.

Indonesian demand for ICT

In 2012, the Internet overtook newspapers to become the second largest medium in the country (after television).[10] Although the number of Internet users, on average, remains low by global standards, they are also estimated to grow rapidly. According to the Indonesian Internet Service Provider Association (APJII), the number of Internet users in 2012 reached 63m, or about 24% of the population. In 2013, the numbers are estimated to increase to 82m users or 30% of the population and continue to grow to 139m and 50% by 2015.[11]

Accenture, a consultancy, has identified four factors behind the Indonesian surge towards a digital society:[12] The economy (which is forecast to grow by 6.4% annually between 2010 and 2020), urbanisation, a youthful population, and the growth in mobile devices.

[9] Indonesia, Masterplan for Acceleration and Expansion of Indonesia Economic Development 2011-2025: http://www.depkeu.go.id/ind/others/bakohumas/bakohumaskemenkoPDFCompleteToPrint%2824Mei%29.pdf
[10] The Jakarta Post: http://www.thejakartapost.com/news/2012/06/27/internet-usurps-press-radio-audience-reach.html
[11] Indonesia Internet Service Provider Association: http://www.apjii.or.id/v2/index.php/read/content/apjii-at-media/139/2013-pengguna-internet-indonesia-bisa-tembus-82-ju.html
[12] Accenture, Ready for Indonesia's digital future?: http://www.accenture.com/Microsites/management-consulting-innovation-center/Documents/pdf/Accenture-ASEAN-Digi-Indonesia-v22-Final.pdf

Indonesian supply of ICT

Indonesia is rated around the world average in both the UN and WEF reports, which measure ICT supply and the extent to which they are leveraged. But the country appears keen on improving. Besides the plan to enhance ICT infrastructure, as described in MP3EI, there is also an effort to increase the supply of information. For example, the availability of online public services along with efforts to improve user access to them, are among the top five priorities for the Ministry of Communication and Information Technology, commonly known as KOMINFO, between 2010 and 2014.[13] "The primary interest for local government institutions in particular is in improving their connections and bandwidth," says Bambang Heru, Director at KOMINFO's Directorate of Information Security. "They are not concerned with cyber security."

The local push for online content is illustrated in a recent report that found several examples and innovative uses of social media in the supply of information by local stakeholders throughout Indonesia, including blogging networks, NGO efforts to use ICTs, citizen journalism as well as new initiatives by traditional media and local governments to reap the benefits of technology.[14]

[13] KOMINFO: http://web.kominfo.go.id/sites/default/files/Prioritas%20Kominfo%20210-214.pdf

[14] Internews, Indonesia: New digital nation?: http://www.internews.org/sites/default/files/resources/Internews_Indonesia_DigitalNation_2012-07.pdf

2 Dependency and its consequences

A growing reliance on ICTs also means an increase in risk. This section offers an overview of cyber threats, both globally as well as those particularly relevant in the Indonesian context. “As the country moves towards a world of electronic payments and e-commerce, cyber attacks can have a significant ramification on society,” says Benjamin Keller, Vice President of Service Operations at XL, an Indonesian telecommunications company. "Therefore, cyber security is in everyone’s best interest.”

“As the country moves towards a world of electronic payments and e-commerce, cyber attacks can have a significant ramification on society”

The potential consequences vary, depending on the threat and the target’s cyber dependency or level of development. Estimating financial loss is a complex task and despite renewed efforts to determine the costs of cyber crime, one can only approximate the figure for Indonesia based on global studies.

Socio-economic implications

Distributed denial of service (DDoS) attacks, a threat designed to overwhelm website(s) with requests to make them unavailable, targeted American and South Korean websites in July 2009. Besides affecting South Korea’s Ministry of Defence, National Congress and financial services institutions, the incident generated pan-Asian interest as many came to see the potential socio-economic implications with such rising threats. It led to the release of Japan’s “Information Security Strategy to Protect the Nation” on May 11, 2010, which explained: “The large-scale cyber attack in the United States and South Korea particularly alerted Japan — where many aspects of economic activities and social life are increasingly dependent upon Information and Communication Technology (ICT) — to the fact that a threat to information security could be a threat to national security and require effective crisis management.”[15]

The potential consequences of attack will grow as countries reach higher levels of development and become increasingly reliant on ICTs. Although the impact of cyber threats is currently unlikely to be catastrophic, argues a recent study on the OECD member states, they can still cause a great deal of harm or have severe financial implications.[16] “In the medium to long-term, OECD member states have to take it seriously,” says Ian Brown, one of the co-authors of the report, and an Associate Director in the Cyber Security

[15] NISC, Information Security Strategy for Protecting the Nation: http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

[16] Ian Brown and Peter Sommer, Reducing Systemic Cybersecurity Risk: http://www.oecd.org/dataoecd/57/44/46889922.pdf

Centre at the University of Oxford. “The scale of the problem is growing,” agrees Ms Kroes. “The biggest concern is that most people and organisations are lacking preparation and often aren’t sure how to prepare.”

Scale of the problem

Estimates of the problem vary depending on definitions, a country’s level of development, and the type and size of the organisation involved, among many other variables. However, previous studies from Symantec, a security company, and the Ponemon Institute, a consultancy, indicate that about 75% of organisations suffer from some sort of cyber attack or breach every year.[17] More recently, Symantec’s 2012 State of Information Survey, which surveyed 4,506 business executives across 38 countries, found that 69% of organisations had experienced an information loss in the past year and had confidential information exposed.[18] Attacks can also compromise trust. Only 12% of European users feel completely safe when making online transactions, according to the Digital Agenda website.

Defining cyber security

Cyber security can be defined in many ways. Viewing it simply as a technological challenge would be limiting. Today, therefore, most people take a broader perspective to account for trends such as the increasingly blurring line of what constitutes crime vs crime that is committed online with offline consequences and the potential responses to such threats which can include both online and offline components. A commonly cited definition is provided by the ITU:[19]

Cybersecurity is 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 organisation and user’s assets. Organisation 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 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

This report defines cyber security in similarly broad terms. In this effort, it considers fixed and mobile networks and devices of equal importance; it also accounts for both hardware and software across the public and private sectors, as well as civil society.

[17] Symantec, State of Enterprise Security and Ponemon Institute, Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government

[18] Symantec, 2012 State of Information Survey:
http://www.symantec.com/about/news/theme jsp?themeid=state-of-information

[19] International Telecommunication Union, ITU-T Recommendation X.1205:
http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1205

Global cyber threats

ICTs have given rise to new opportunities but digital tools have simultaneously created new targets for attack. The range and nature of cyber threats vary greatly and can have both online and offline consequences. Following is an overview of various global cyber threats across two broad categories: those with a political motive and those without.

Politically motivated threats

A common objective for politically motivated cyber threats is generally to compromise the integrity and availability of information for political purposes, whether the attacker is a nation-state, a group, or a single individual.

Many consider the purported Russian DDoS attacks on Estonia in April 2007 as an example of the first cyber war, although it is probably more appropriately labeled as a web-war or cyber terrorism since offline consequences were limited and no physical damage occurred. The attacks were carried out using a botnet, which is a collection of computers controlled remotely that can overwhelm web servers, rendering them unavailable. To distinguish such attacks from more serious ones, cyber warfare often indicates a cyber attack with offline consequences to critical infrastructures. In 2010, for example, Stuxnet, a malicious software, or malware as it is commonly known, reportedly succeeded in physically disrupting Iran's nuclear power reactors. Given the sophistication needed, attacks with such consequences are rare but increasingly likely as countries invest in cyber attack capabilities and consider disruption through cyber means as a potential alternative to diplomacy or traditional military action.

Cyber espionage is similar to offline espionage, in essence to eavesdrop or steal information without being detected. In the private sector, it would be labeled corporate espionage and considered a cyber crime (see next section) but when countries or individuals are targeted, the motivation is primarily political. Several high-profile incidents have been uncovered in recent years, although the perpetrators are rarely identified. In 2008, for example, Ronald Deibert of University of Toronto and Rafal Rohosinski of SecDev Group, a consultancy, uncovered a malware which was remotely controlled to send information to a secret location without duplicating itself like traditional viruses. About one-third of the infected computers are said to be high value targets and the perpetrators were never discovered. In August 2011, McAfee, a security company, uncovered an espionage program, termed Operation Shady RAT, which was designed to steal information from corporations and governments alike.

Hacktivism, a term that combines "hacking" and "activist," is different from other types of politically motivated threats because the attackers often seek to maximise publicity in order to send a political message. This is commonly done by de-facing a website, meaning it is given a new appearance by the perpetrators such as providing a simple message taking credit for the attack, or by blocking access to it using a DDoS attack. In recent years, the most commonly cited examples of this type of attack come from Anonymous, a group which supports free speech and have been vocal in their support of WikiLeaks, the whistleblowing website. In 2010, for example, Anonymous launched “Operation Payback,” during which it used DDoS attacks to shut down websites that supported censorship of WikiLeaks, such as those of MasterCard, PayPal and Visa.

As organisations, their customers, and society at large, went online, so too did criminals. ICTs provide a new platform for corporate espionage, intellectual property theft, fraud and various forms of illegal activity. Although there are other non-politically motivated cyber threats, such as disruptive behavior from employees, most threats within this category would fall under the general header of cyber crime and an important distinction from politically motivated threats is that nation-states are unlikely to be behind them and the consequences are primarily economic in nature.

Cyber crime was defined by the 2001 Budapest Convention (formally known as the Council of Europe’s Convention on Cybercrime) as encompassing four categories: offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and, offences related to infringements of copyright and related rights. [20]

In a global study on cyber crime in UN member states, the United Nations Office on Drugs and Crime (UNODC) found that, overall, countries were equally concerned about three broad categories of threats: attacks on the confidentiality, integrity, and availability of information (CIA model); financially-driven threats, such as fraud, forgery and phishing; and, content-related crimes.[21] Although regional differences are small, there is one discernable trend: In lesser developed countries, law enforcement encounter acts against the CIA model less frequently whereas in more developed countries, there appears to be an equal distribution among the three.

Today, the cost of financial cyber crimes is reaching new proportions, in particular for countries and corporations that are heavily cyber dependent (for details, see next section). For example, in 2011, SONY, a media company, informed its 77m online users that their personal information and credit card data may have been compromised by cyber criminals. An online industry website, ZDNet, reported that the legal fees, support and lost revenue from this breach alone would amount to a minimum of USD 171m.

[20] Council of Europe, Convention on Cybercrime:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[21] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime:
http://www.unodc.org/unodc/en/organised-crime/expert-group-to-conduct-study-cybercrime-feb-2013.html

Table 1: A summary of threats

Politically motivated threats	Description	Example(s)
Cyber warfare and cyber terrorism	Attacks by nation-states or highly sophisticated groups that target the availability and integrity of data, potentially with physical consequences	Estonia; Stuxnet
Cyber espionage	Theft of information that compromises confidentiality	GhostNet; Shady RAT
Hacktivism	Defacing websites or blocking access to them through DDoS attacks to send a political message	Anonymous
Non-politically motivated threats	**Description**	**Example(s)**
Cyber crime, such as corporate espionage, intellectual property theft, identity theft, fraud	Typically financially motivated crimes based on data that is often stolen through malware and phishing techniques in which users click on unknown links; methods also include hacking for information or collecting it on commonly used platforms, such as social media websites	SONY

Source: Author compilation based on an adaptation from Kim Andreasson, editor, Cybersecurity: Public Sector Threats and Responses.

Cyber threats to Indonesia

Global threats are equally applicable to Indonesia; however, some aspects of the country's Internet usage make it more vulnerable to certain types of attacks. For example, given its level of development, Indonesia does not appear to be particularly susceptible to politically motivated cyber threats. The country is currently in the information awareness stage and has yet to develop offensive or defensive military cyber capabilities (although it appears to be in the early stages of doing so). It is also unlikely to be a target of cyber warfare, terrorism or espionage activities in the near future as attackers would have little to gain. However, as Indonesia progresses and becomes increasingly cyber dependent, it is likely these threats will increase in the medium- to long-term.

Politically motivated attacks currently appear limited to hacktivism, including most recently in early 2013 when prominent government websites were defaced. "The number is high," says Budi Rahardjo at the Indonesia Computer Emergency Response Team (ID-CERT), "but fortunately, most of these are just digital graffiti."

Cyber crime in Indonesia

Indonesia appears more susceptible than many other countries to cyber crimes such as fraud and content-related challenges, which is indicative of the level of ICT development in which the country finds itself. For example, although Mr Rahardjo, who also teaches at the Bandung Institute of Technology and is the founder of PT INDOCISC, a network and application security company, says corporate espionage is on the rise, foreign attacks on the Indonesian private sector is currently of limited value compared to more developed nations, which means they are also less likely to occur on a relative basis.

Instead, Indonesia today is primarily a target for less sophisticated cyber crimes in which the attackers prey on the lack of awareness among people to seek financial gain. Indicative of this, Indonesia ranked tenth in Symantec's global list as the country accounted for 2.4% of the world's cyber crimes in 2011.[22] According to Rudi Lumanto, Chairman of the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), data show there were about 39m attacks in the past year. Of those, 35% originated from outside the country while 65% came from within.

In general, there appears to be five particular areas of concern or vulnerability in Indonesia today; they are (in no particular order):

Malware

According to the threat exposure rate (TER) in the Security Threat Report 2013 from Sophos, a security firm, at 23.54%, Indonesia had the highest percentage of PCs that experienced a malware attack in the world over a three month period (China was second with 21.26%; Norway and Sweden the lowest with 1.81% and 2.59% respectively).[23]

"There is a lack of awareness"

"There is a lack of awareness," says Yudhistira Nugraha, Head of Information Security Risk Management at the Directorate of Information Security. Because of this, malware is a particular problem in Indonesia along with spam and other types of email-based scams, he says. Although threats vary depending on the type of organisation or person targeted, Mr Rahardjo agrees that malware and phishing are generally the biggest concerns in Indonesia today.

Phishing

Although phishing overlaps somewhat with malware, several interviewees point to social engineering emails as a particularly troubling trend. Jaziar Radianti, an Indonesian who is now a Post-Doctoral researcher at the University of Agder in Norway, says it is one of the biggest problems because people actually tend to provide their personal information in response to such emails.

"Unfortunately users are not equipped with sufficient knowledge about IT, especially IT security, which makes them vulnerable to cyber crime using social engineering techniques," agrees Mohammad Guntur, Senior Vice President of IT Strategy, Architecture & Planning Group at Bank Mandiri. "Very often

[22] The Jakarta Post: http://www.thejakartapost.com/news/2012/05/16/indonesia-ranks-tenth-world-cyber-criminality.html

[23] Sophos, Security Threat Report 2013: http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2013.pdf

these novices are deceived by fake website, phishing email, sms-phishing (smishing), etc."

Mobile threats

"Phishing is an enormous problem," agrees Mr Keller at XL, who also points out that the technique is spreading to mobile devices in the forms of SMS texts. "Perhaps the problem is simple... but the sheer number is the problem," observes Mr Rahardjo. With more mobile devices than there are people, this type of threat is likely to explode in the near future. As people move to mobile, so will criminals.

"Perhaps the problem is simple... but the sheer number is the problem"

According to Nielsen, a research firm, almost half of Indonesia's population browses the Internet via mobile phones, which is the highest mobile Internet dependency in Southeast Asia.[24] At the same time, the 2012 Norton cybercrime report say the rise of mobile access is a particular problem as people don't use a security solution for their devices; in fact, almost half (44%) of those surveyed globally aren't even aware that they exist. [25]

Social media

Due to the popularity of social media platforms, users in Indonesia may be particularly targeted by criminals looking to collect information in order to build profiles on them. Data from TNS, a market research company, show that 87% of Indonesians who go online have a social media account.[26] "Facebook is very popular but there is little mentioning of the kinds of security risks that come with it and people are not so much aware," says Ms Radianti as she compares security awareness in her native Indonesia to her adopted Norway. In Indonesia, many people put all their information – everything – on Facebook, says Mr Nugraha. At the same time, data from the 2012 Norton cybercrime report shows that 4 in 10 social network users globally have been victims of a cyber crime on those platforms.

"Facebook is very popular but there is little mentioning of the kinds of security risks that come with it and people are not so much aware"

Compounding the problem, Mr Lumanto points out that 87% of Indonesia's Facebook and Twitter traffic comes from mobile devices. "And as with any mobile users in the world, the concern to security is very low," he says.

Hacktivism

Cyber crimes dominate current concerns; the lone exception is the defacement of primarily government websites, which can qualify as an offence with political motifs (although it can also be seen as a crime from a law enforcement perspective, particularly when conducted by so-called "script kiddies" that are defacing high-profile websites for the fun of it). This is still the most common cyber security problem in Indonesia today, says IGN Mantra, Chairman of the Indonesia Academic CSIRT/CERT. "Everyday the sites have been hacked."

"Everyday the sites have been hacked"

[24] The Jakarta Post: http://www.thejakartapost.com/news/2011/07/12/ri-highly-dependent-mobile-internet.html

[25] Norton, 2012 Cybercrime Report: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[26] The Jakarta Post: http://www.thejakartapost.com/news/2011/05/31/cheap-smartphones-change-ri-internet-behavior-survey.html

The numbers prove his point. Between 1 January 2013 until mid-February 2013, 60% of attacks on government domains were web defacements (followed by malware attacks at 36%), according to a Government CSIRT (Gov-CSIRT) report.[27]

Although hacktivism is more of a nuisance than a threat per se, it still causes trouble. In early January 2013, the official website of Indonesian president Susilo Bambang Yudhoyono, presidensby.info, was defaced.[28] After the arrest of the suspect, more government websites were attacked in retaliation.[29]

The cost of cyber crime in the world and in Indonesia

The cost of cyber crime is inherently difficult, if not impossible, to calculate appropriately and any estimate requires a number of assumptions. “The cost of cyber security can vary depending on the size of the organisation and the risks it faces, which in turn depend on a number of factors,” says Ms Kroes. For example, how can one accurately quantify the loss of trust or loss of future business opportunities due to cyber crime headlines in newspapers? This section discusses commonly cited models in attempting to estimate financial loss from cyber crime and their inherent limitations before applying them to Indonesia.

> “The cost of cyber security can vary depending on the size of the organisation and the risks it faces, which in turn depend on a number of factors”

Questions linger

A commonly cited figure for financial loss is the Norton cyber crime report from Symantec. According to the 2012 edition, based on a survey of 13,018 online adults aged 18-64 across 24 countries, it estimates the global cost of consumer cyber crime at USD 110bn annually.[30] It also notes that almost half (46%) of the adult online population surveyed have been victims to some sort of attack, defined as everything from malware and viruses to fraud and theft.

Although everyone realises the difficulty of measuring the true costs of cyber crime, many figures appear widely overestimated.[31] A report by Detica, a software security company that is part of BAE Systems, the defence company, estimated the cost of cyber crime in the UK at GBP 27bn, or 1.8% of its GDP. [32] In part because of doubts surrounding this number, the UK’s Ministry of Defence commissioned an independent study to assess it. The resulting Ross Anderson, et al, report on “Measuring the Cost of Cybercrime” is widely recognised as the best available estimate as of this writing, although it declines to give a total figure for the cost of cyber crime to the world or to the UK, as “it is entirely misleading to provide totals lest they be quoted out of context, without all the caveats and cautions that we have provided.”[33]

[27] GovCSIRT, Report 2012 – 2013.

[28] E Hacking News: http://www.ehackingnews.com/2013/01/indonesian-president-website-hacked-by.html

[29] Jakarta Globe: http://www.thejakartaglobe.com/home/govt-sites-hacked-following-arrest-of-alleged-jember-hacker/568523

[30] Norton, 2012 Cybercrime Report: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[31] Network World: http: //www.networkworld.com/news/2012/082912-oft-cited-cybercrime-cost-estimates-hosed-262021.html

[32] The Economist: http://www.economist.com/node/21557817

[33] Ross Anderson, et al, Measuring the Cost of Cybercrime: http:/ weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

A lack of numbers in Indonesia too

As elsewhere in the world, the true cost of cyber crime in Indonesia is unknown. “ID-CERT has tried to collect this kind of information from public sources. The number is low. This is due to the fact that most (all?) cases that are related to financial fraud are not reported formally,” says Mr Rahardjo. Indicative of this grey area, the Threat and Vulnerability report from ID-SIRTII states that in 2011, the total financial loss from fraud was reported at USD 65,040.[34]

The cost of cyber crime also goes beyond numbers. “For financial institutions such as banks, cyber security must be carried out at any cost because banking is a ‘trust’ business,” says Mr Guntur. Such indirect costs are probably impossible to quantify. Budgets are easier, although they may not mean much, especially in the case of government as they are low. Mr Lumanto says the total budget for the Ministry of Communication and Information Technology in 2013 is around USD 400m; the cyber security portion of that is around USD 4.1m or only 1% of the total budget. “In most cases, the cost for recovery is much higher than the cost for preventive actions,” he adds.

> “For financial institutions such as banks, cyber security must be carried out at any cost because banking is a ‘trust’ business”

Estimating the cost of cyber crime in Indonesia

Despite the fact that they are often criticised, estimates of the cost of cyber crime are frequently used to derive at potential financial implications due to the lack of hard data. The recent UNODC Study on Cybercrime, for example, took the Ross Anderson, et al, and Norton studies, and compared them at country level in order to identify broad patterns. Although such estimates need to be interpreted with great care as they can vary massively depending on indirect cost, they give an indication (albeit a broad one), of potential cost. This report takes a similar view and uses the same methodologies in order to derive estimates for the cost of cyber crime in Indonesia specifically.

The cost, using the Norton survey

The USD 110bn cost of consumer cyber crime reported by Norton is derived according to an estimate of 556m victims, which means the average global cost per victim is USD 197.[35] Because there does not appear to be any reliable sources for the average cost of cyber crime per victim in Indonesia, the figures from the Norton report are used here. Further, according to news reports in 2010, approximately 86% of Internet users in Indonesia are victims of cyber crimes, a figure that seems high although it is also reported that Indonesia is more prone to cyber crimes than most other countries.[36] Taking the average global cost per victim from Norton and the reported number of Internet users in Indonesia, 63m, the estimate for the annual cost of cyber crime in the country is USD 10.7bn (63m Internet users * 86% victimisation rate = 54.2m victims of cybercrime; 54.2m victims * USD 197 average loss per victim = USD 10.7bn). The lowest reported direct loss estimate from the Norton study was USD 50. Using this figure, a lower bound estimate for the cost of cyber crime in Indonesia is USD 2.7bn (54.2m victims * USD 50 = USD 2.7bn).

[34] ID-SIRTII, Threat and Vulnerability in Indonesia.

[35] Norton, 2012 Cybercrime Report:
http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[36] VIVAnews:
http://us.en.news.viva.co.id/news/read/180175-cyber-crime-attacks-86--indonesia-s-users

The reported percentage of Internet users subject to cyber crimes is difficult to verify and may be significantly lower. As such, table 2 provides the potential cost depending on the rate of victimisation:

Table 2: Victimisation rates and estimates of cyber crime cost in Indonesia

Victimisation rate:	25%	50%	75%
Estimated number of victims:*	15.7m	31.5m	47.3m
Estimated low cost:**	USD 788m	USD 1,575m	USD 2,363m
Estimated average cost:**	USD 3,099m	USD 6,199m	USD 9,298m

*Sources: *Based on usage estimates from APJII. **Based on Norton estimates.*

The cost, using the Anderson, et al, model

Anderson, et al, do not add up the total cost of cyber crime; instead, it uses "the best figures from current research" to estimate global costs over four categories: genuine cyber crime; transitional cyber crime; cyber criminal infrastructure; and traditional crimes becoming cyber. When figures were unavailable, they were estimated using the UK's GDP as a per cent of the global economy. Since there does not appear to be any data for Indonesia on any particular line item, costs are estimated here by using Indonesia's GDP as a per cent of the global economy.

Table 3: Estimates of cyber crime cost in the world and Indonesia

	Global	Indonesia
GDP:*	USD 71, 620bn	USD 895bn
Per cent of global GDP*:		1,20%
Cost of:**		
Genuine cybercrime:	USD 3,457m	USD 43m
Transitional cybercrime:	USD 46,600m	USD 582m
Cybercriminal infrastructure:	USD 24,840m	USD 310m
Traditional crimes becoming cyber:	USD 150,200m	USD 2,748m

*Sources: *CIA World Factbook. **Based on Anderson, et al, model.*

As elsewhere in the world, the estimates derived here come with a number of assumptions and should be interpreted with great caution; however, if they are anywhere near the true cost of cyber crime in Indonesia, they do indicate a strong need for enhancing cyber preparedness.

3 The state of cyber security

The level of cyber security preparedness – between countries but also within them – varies greatly. Although there is general agreement on the importance of global coordination, cyber security remains a nation-state issue where individual organisations are often the first line of defence. This section illustrates current international responses as well as the state of cyber security in Indonesia specifically.

Global initiatives

Recalling the classification of cyber threats as either politically motivated or criminal and non-political in nature, one can see that cross-national initiatives focus on the latter. Despite recent calls for agreements on international law or norms for behavior when it comes to political attacks, such as cyber warfare, terrorism, and espionage, decisions regarding their use remain firmly within the auspices of individual nation-states. The lone exception is occasional international cooperation in regards to hacktivism as many countries share the view that they are also criminal acts as seen during crackdowns on WikiLeaks and Anonymous. For threats classified as cyber crime and other non-political motives, there are a large number of initiatives, an overview of which follows.

UN resolutions

The UN General Assembly has addressed cyber crime primarily through resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, which together with other relevant resolutions, urges member states to consider the multi-lateral dimensions of threats in the usage of ICTs, as well as proposing measures to limit them.

ITU and UNODC

As the UN specialised agency for ICTs, ITU is the global lead for cyber security.[37] Of particular note is the agency's development of the Global Cybersecurity Agenda (GCA), a framework to help countries take national measures and also harmonise them at the international level. The five pillars of the GCA are: legal measures; technical and procedural measures; organisational structures; capacity building; and international cooperation. The UNODC, meanwhile, leads the UN efforts against an "uncivil society," which includes organised crime and terrorism, hence it is also tasked with combating cyber crime.

[37] "Building confidence and security in the use of ICTs," known as Action Line C5, was established at the second World Summit on the Information Society (WSIS) in Tunis, Tunisia, in November 2005.

International Multilateral Partnership Against Cyber Threats (IMPACT)

In 2011, IMPACT officially became the cyber security executing arm for the ITU and is tasked with providing access to expertise and information through the Global Response Centre (GRC) which helps realise the GCA through NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for Experts). With 145 nations as members, it is the world's largest cyber security alliance.[38]

Budapest Convention

As mentioned, the Convention is commonly used as the standard definition of cyber crime, particularly its substantive criminal law section.[39] As of September 2012, 37 countries had ratified its use.

Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT)

CERT and CSIRT fulfill the same function as they are both designated to handle computer security incidents. The approach was established at Carnegie Mellon University in 1988 and today most countries have a CERT, sometimes affiliated with the government and sometimes not.

Forum for Incident Response and Security Teams (FIRST)

Founded in 1990, FIRST provides a platform for members to deal more effectively with security incidents by offering information on best practices and access to various tools.[40] The organisation consists of incident response teams across the world from a wide variety of actors, including the public and private sectors, as well as academia.

Regional and national measures

Regional legal frameworks include the Council of Europe Convention (above), as well as the Arab League model law, Commonwealth model law[41], the Economic Community of West African States (ECOWAS) Directive[42], and the Draft African Union Convention.[43]

In the Asia-Pacific region, CSIRTs collaborate through APCERT (Asia-Pacific Computer Emergency Response Team). In addition, the region benefits from the work of the Asia-Pacific Economic Cooperation (APEC) whose Strategic Plan for 2010-2015 includes, as a priority area, the development of ICT to enhance socio-economic growth while providing a safe digital environment and improving regional cooperation.[44]

[38] IMPACT: http://www.impact-alliance.org

[39] Council of Europe, Convention on Cybercrime:
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[40] FIRST: http://www.first.org

[41] Commonwealth model law:
http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf

[42] ECOWAS : http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/documents-ecowas.html

[43] African Union Convention background information available at:
http://www.au.int/pages/infosoc/pages/cyber-security
For the draft convention: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

[44] APEC, Strategic Plan for 2010-2015:
http://www.apec.org/Home/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information

Individual countries have taken different approaches to cyber security, although one can argue that development generally occurs across three broad categories. The first are those that have recognised the tie between ICT and socio-economic growth and made that explicit as part of the country's national strategy, development agenda, or equivalent document. This often leads to a second effort to secure the civilian cyberspace to sustain those benefits, such as the National Security Strategy in the UK which highlights cyber attack by other states, terrorists or organised crime groups as one of the four highest risks to the country.[45] Although there is some overlap, the third category consists of those that have expressly established military capabilities in cyberspace, such as the US.[46]

[45] UK, A Strong Britain in an Age of Uncertainty:
http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

[46] The first US Cybercom Commander was appointed in May 2010:
http://www.defence.gov/releases/release.aspx?releaseid=13551

4 The Indonesian response

Information security awareness in Indonesia is limited and also reflected in the types of threats to which it is said to be particularly vulnerable. Compared to the three broad categories of national-level responses, Indonesia has recognised the tie between ICT and socio-economic growth but it has yet to develop a civilian cyber security strategy or a military doctrine, although initial steps are being taken in both areas. This section discusses the current cyber security efforts in Indonesia.

Legislative initiatives

The legal foundation for cyber security in Indonesia is weak. There are only two Acts that deal with the topic and they both have their limits. The Telecommunication Act, No. 36/1999, only mentions telecommunications infrastructure security briefly and does not discuss it in the context of the Internet specifically. The more recent Information and Transaction Electronic Act, No. 11/2008, provides the basis for law enforcement in regards to cyber crime; however, it is limited in scope and other Acts are often used to supplement it in order to prosecute criminals, such as the Copyright Act, No. 19/2002 and the Pornography Act, No. 44/2008. Most recently, the government issued the Electronic System Provider and Electronic Transaction Regulation No. 82/2012 in which every provider of such services must register with KOMINFO.

Key stakeholders

When it comes to cyber security, everyone is a stakeholder. From public sector entities to the private sector and civil society, this section introduces a selection of key stakeholders in Indonesia. It is particularly important in the local context as each institution or group of institutions are encouraged to develop their own CERT/CSIRT.[47] Based on such recommendation, academic institutions have formed an Academic CSIRT, and other groups are in the process of following their lead. “As long as the attack is limited in scope (not a national threat), then each CERT or group CERT will handle it by themselves,” explains Yudho Giri Sucahyo, Professor in the Faculty of Computer Science at the University of Indonesia. If it is a national threat, KOMINFO is the lead organisation regarding civil cyber security while threats that concern national security also involve the Ministry of Defence.

[47] KOMINFO:
http://event.idsirtii.or.id/wp-content/uploads/2011/10/Cyber-Security-Ecosystem-Ministryof-Communication-and-Information-Technology-email.pdf

Ministry of Communication and Information Technology (KOMINFO)
Organisationally, KOMINFO is divided into five areas: Directorate General (DG) of Post and Information Technology Implementation, DG of Information and Public Communication, Human Resources Research and Development Agency, DG of Post and Information Technology's Resources and Tools, and the DG of Information Technology's Application, the latter of which is particularly relevant to cyber security as it is home to the Directorate of Information Security.

The Directorate of Information Security in turn consists of five Information Security divisions. The first is the division for Governance, which deals with policy, regulation, and standards. The division of Technology, as the name implies, deals with such issues as how to implement secure information security technology. The Gov-CSIRT falls under the division of Monitoring, Evaluation and Incident Response. The division of Forensic and Law Enforcement is self-explanatory while the division of Culture is enhancing knowledge. "We are now starting the socialisation of information security awareness," says Mr Heru, the Director of the Directorate of Information Security. His budget for 2013 is about 20bn Rupiah or about USD 2m, up from 17bn Rupiah in 2012, and he employs a staff of about 35.

"We are now starting the socialisation of information security awareness"

There is a direct line between Mr Heru and ID-SIRTII, which has two distinct functions.[48] First, it monitors and provides an early warning system of threats in Indonesia and take measures to counter them when needed. Secondly, it offers educational activities to improve handling of security incidents. For example, it provides training courses on how to develop a CERT/CSIRT. In 2011, it helped launch the Academic CSIRT and last year the Gov-CSIRT. According to Mr Lumanto, its Chairman, it is currently supporting the Ministry of Defence in preparing a Military CSIRT. The annual budget for ID-SIRTII was initially less than 10bn Rupiah when it was established in 2007; however, in the last three years the annual budget has averaged around 19bn Rupiah, according to Mr Lumanto.

CERTs/CSIRTs
Based on overall strategy, ID-SIRTII is helping institutions or group of institutions to develop their on CERT/CSIRT. The first of those was the Academic CSIRT. "Our strategy is to protect campus assets, such as databases and web servers as well as to provide awareness to the students about cyber security," says Mr Mantra, its Chairman. To do so, he has an annual budget of about 1bn Rupiah or about USD 100,000. With 50 academic institutions as members, it means that each pay about USD 2,000.

The objective of the Gov-CSIRT is similarly to work with a range of stakeholders to improve information security for its government members by providing them with a platform for sharing of information and incident handling.[49] Organisationally, it falls under the Directorate of Information Security and logistically it consists of a general manager with teams for monitoring, evaluation and incident response. Membership is open to all government entities and

[48] ID-SIRTII: http://idsirtii.or.id
[49] Gov-CSIRT: http://insting.kominfo.go.id/tentang-idgovcert/rfc-2350/

is currently composed of 161 central government agencies, 33 provincial government entities and 497 local governments.[50]

Internationally, ID-SIRTII and ID-CERT are both full members of the AP-CERT, which supports Internet security throughout the Asia-Pacific region.[51] ID-SIRTII is also a Full Member of the Organisation of the Islamic Conference-CERT (OIC-CERT), which provides a platform for its members to develop collaborative approaches to improve cyber security.[52]

Ministry of Foreign Affairs

“Since we [Indonesia] have other agencies handling the technical aspects, we first and foremost try to support them from a policy perspective and make cyber more of a priority,” says Daniel TS Simanjuntak, the Deputy Director for WMD and Conventional Weapons at the Ministry of Foreign Affairs. To do so, the Ministry of Foreign Affairs work with domestic institutions to outline a potential national policy beyond cyber crime, i.e. policy on cyber security.

> “Since we [Indonesia] have other agencies handling the technical aspects, we first and foremost try to support them from a policy perspective and make cyber more of a priority”

The second broad category of work, given its obvious remit, entails the global aspects of cyber security. The Ministry is looking to enhance the level of international dialogue and identify the relevant platforms in which to address cyber security. “We are looking for opportunities in various international forums to see how Indonesia can play an active part in developing a comprehensive future direction of cyber security,” says Mr Simanjuntak.

Ministry of Defence

As elsewhere in the world, cyber security in Indonesia is both a national civilian concern and a topic of interest to the national security community, often led by the Ministry of Defence. Although countries point to its defensive necessities, there is in effect a global cyber arms race at the moment and nobody wants to be left behind (for good reason).

Indonesia is no different. In November 2012, Deputy Defence Minister, Sjafrie Sjamsoeddin, announced that the country will establish a cyber defence unit, which will be dedicated to securing military systems and national IT infrastructure.[53] The cyber defence operations centre (CDOC) is meant to work closely with an already established cyber defence task force operated by the Indonesian Armed Forces. According to reports, it also expects CDOC to develop a national doctrine on cyber security.

Indonesian Police

A 2010 presentation entitled “Current state of cybersecurity readiness and cybercrime enforcement capability in Indonesia,” outlined numerous challenges facing the Indonesian Police.[54]

[50] Presentation by Yudhistira Nugraha at the 3rd annual Cyber Security for Government Asia conference in Kuala Lumpur, Malaysia, on 29 January 2013.

[51] APCERT: http://www.apcert.org

[52] OIC-CERT: http://www.oic-cert.net

[53] IHS Jane’s: http://www.janes.com/products/janes/defence-security-report.aspx?id=1065973890

[54] Presentation by Ratno Kuncoro at the Cybercrime Capacity Building Conference in the State of Brunei Darussalam, 27-28 April 2010: http://aseanregionalforum.asean.org/files/Archive/17th/ARF-Cybercrime-Capacity-Building-Conference-BSB-27-28April2010/Annex%208%20-%20Indonesia%20-%20cybersecurity%20and%20cybercrime.pdf

As the Head of IT & Cyber Crime Section, Police Colonel Winston Tommy Watuliu probably knows better than anyone what needs to be done to improve the situation. "We still need to update regulations," he says. Examples include problems in the identification of users and making spam as part of the penal code.

"We still need to update regulations"

Further, although Mr Watuliu calls his department's relationship with prosecutors, and private sector organisations, such as ISPs and telecommunications operators "good," he would also like to strengthen the collaboration regarding skills development and establish a common understanding of cyber crime. Benedicta Kristanti, Officer for Counter-Terrorism at the Ministry of Foreign Affairs, agrees that Indonesia should develop capacity building programmes for prosecutors and judges regarding the criminal proceeding process related to cyber crime, particularly for the use of electronic evidence.

The private sector

The civilian cyber security response benefits from cooperation between sectors, which has long resulted in the establishment of various forms of public-private partnerships (PPPs). In Indonesia, as elsewhere, there are lingering questions surrounding their effectiveness (see box on page 30 for the global debate). "They have not worked optimally," says Mr Lumanto at ID-SIRTII, "because there is a gap in security understanding between the public and private sectors," a point that reinforces the notion of Mr Watuliu.

Despite some issues, however, all participants agree on one thing: the importance of taking a multi-stakeholder approach to cyber security. The Indonesian government realises that many critical infrastructures are owned and operated by the private sector while local companies recognise the need for cooperation.

At Bank Mandiri, Mr Guntur remains positive towards PPPs. They can bring great advantages, although he says the least successful strategy towards cyber security is one that relies on people because then it depends on their awareness. Instead, Mr Guntur suggests a strategy based on technology, such as security tokens, best-of-breed IT infrastructure, systems and applications. It remains to be seen whether such approach can be applied to PPPs.

But just as the public and private sectors as well as civil society all benefit from ICTs, they also all stand to have something to lose to cyber threats. Therefore, the necessity to find a way to collaborate and give everyone a voice in cyber security continues, here and elsewhere.

Academia and civil society

Everyone can contribute to cyber security, perhaps particularly in terms of awareness, and as the public and private sectors face limitations, others can help. "Academia and civil society can contribute to cyber security by increasing security awareness and building a security culture," says Mr Rahardjo, who founded ID-CERT in 1998 and later took part in the founding of APCERT.[55]

"Academia and civil society can contribute to cyber security by increasing security awareness and building a security culture"

[55] ID-CERT: http://www.cert.or.id

ID-CERT is an NGO, which can only provide information of incidents and relies entirely on the cooperation of others in handling them. But with academic, public and private sector members, it also represents a broad community that undertakes research and promotes security awareness to the benefit of all.

Another successful civil society initiative is the Indonesian ICT Partnership Association (ICT Watch), an NGO founded in 2002 that promotes safer Internet use, primarily through its "Healthy Internet" programme, which is now adopted by parties around Indonesia.[56]

PPPs and regulation vs self-governance: A global debate

"PPPs haven't worked because they [the private sector] don't self-regulate; we have been trying this for 10+ years now," says Mr Brown, although he admits that governments should work with the private sector as far as possible before starting to regulate.

"We work with specific government bodies more from a coordination standpoint," agrees Simon Mui, Head of Subsidiaries and Acquisitions, Group Information Security at Standard Chartered Bank.

Two reports from the General Accountability Office in the US also illustrate the limits of PPPs: "Without improvements in meeting private and public stakeholder expectations, the partnership will remain less than optimal, and there is a risk that owners and operators of critical infrastructure will not have the appropriate information and mechanisms to thwart sophisticated cyber attacks that could have catastrophic effects on our nation's cyber-reliant critical infrastructure."[57]

In the EU, Ms Kroes, attributes part of the problem to confidentiality concerns. To overcome them, the Commission's new cyber security strategy establishes a new type of public private platform through which industry can voice its concerns, which will allow the public sector to enhance non-regulatory incentives to improve cyber security.

But international companies also encounter yet another problem, which is in keeping up with multiple regulatory regimes across countries and continents through which information flow seamlessly, ironically helped by the very ICT networks that they are asked to protect.

[56] Indonesian ICT Partnership Association (ICT Watch): http://www.ictwatch.com

[57] Government Accountability Office. "Critical Infrastructure Protection: Key Public and Private Cyber Expectations Need to Be Consistently Addressed" (GAO-10-628) and "Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance," (GAO-10-606).

5 The future of cyber security in Indonesia

Digital development marches on. From big data and open data to cloud computing and mobility, government and businesses around the world are increasingly relying on ICTs to improve effectiveness. Thanks to competition and strong user interest, Indonesia is already capturing many of the benefits of mobility, and hence also a disproportionate number of current threats in this area. As the country begins to seize the full benefits of a broader range of ICTs, the risks will also proliferate accordingly.

Opportunities and threats

High socio-economic growth means that the threats will change and new levels of development will create a need for new national priorities. According to MP3EI, its current Masterplan, Indonesia aims to be a developed country by 2025 with expected annual per capita income in the range of USD 14,250 to USD 15,500.

Based on the experience in more developed countries, it is likely that this will lead to an increase in sophisticated threats, including politically motivated attacks and various forms of political and corporate espionage stemming from Advanced Persistent Threats (APTs), which is a highly advanced form of attack often generated by a state or a state-sponsored entity.

“If we don't improve (our capabilities) we could face a possible public and commercial institutional collapse,” one Indonesian official warned in 2011.[58] As a result, Indonesia must do more to promote integration of cyber security, not only into ICT initiatives but also put it into a wider societal context. Such effort begin by identifying the country’s current strengths and weaknesses in this area.

[58] Reuters:
http://www.reuters.com/article/2011/06/14/us-cyberattack-policy-idUSTRE75D1SI20110614

Recent cyber security initiatives

The past 12 months has seen a number of new cyber security initiatives in Indonesia; what follows is a selection.

March 2012: During the FIRST Technical Colloqium meeting in Bali, Marsan A. Iskandar, Chairman of the Agency for the Assessment and Application of Technology (BPPT), calls for a comprehensive and inclusive National Cyber Defence Strategy, which includes all stakeholders in order to strengthen Indonesia's future cyber security.[59]

October 2012: Ministry of Communication and Information Technology (KOMINFO) hosts the Indonesia Information Security Forum (IISF) in Bandung.[60]

October 2012: Indonesia participates in the ASEAN-Japan Information Security Symposium, which includes awareness raising campaigns.[61]

October 2012: Government issues regulation No. 82 of 2012 regarding Electronic Systems and Transactions in which every provider of such services must register with KOMINFO.[62]

November 2012: Deputy Defence Minister, Sjafrie Sjamsoeddin, announces that Indonesia will establish a cyber defence unit.[63]

January 2013: Bandung Institute of Technology in cooperation with Korean International Cooperation Agency (KOICA) build Indonesia's first cyber security centre, which includes research and graduate education.[64]

Strengths and weaknesses

One recent scholarly article, which assesses Indonesia's strengths and weaknesses, used the ITU's five pillars of the GCA as its framework.[65] It's a good approach through which to identify weaknesses and develop a roadmap, says Mr Sucahyo, one of the co-authors. "We are very strong on technical and procedural measures," he adds. International cooperation is also not deemed to be a problem, a point with which Mr Lumanto agrees: "We are also enhancing our international cooperation with many organisations, security experts and forum in order to improve our understanding of global threats."

[59] Presentation by Marsan A. Iskandar at the FIRST Technical Colloqium meeting in Bali, 30 March 2012:
http://event.idsirtii.or.id/wp-content/uploads/2011/10/Indonesian-Cyber-Defence-Initiatives-Dr.-Marsan-A.-Iskandar-BPPT-email.pdf

[60] KOMINFO: http://iisf.kominfo.go.id

[61] NISC: http://www.nisc.go.jp/aj-sec/

[62] Legal500.com: http://www.legal500.com/c/indonesia/developments/22213

[63] IHS Jane's: http://www.janes.com/products/janes/defence-security-report.aspx?id=1065973890

[64] Institut Teknologi Bandung:
http://www.itb.ac.id/en/news/itb_news_3813.pdf and Tempo.co: http://www.tempo.co/read/news/2013/01/30/061457985/ITB-Bangun-Cyber-Security-Center

[65] Farisya Setiadi, Yudho Giri Sucahyo and Sainal A. Hasibuan, An Overview of the Development Indonesia National Cyber Security: http://www.ijitcs.com/icitea2012/Farisya+Setiadi.pdf

Indonesia is particularly weak in legislative measures, says Mr Sucahyo, calling existing ones at an "initial stage." It is a point with which many interviewees for this report agree and Indonesian officials have publicly acknowledged it is vulnerable to cyber threats in part because of weak legislation.[66] Mr Sucahyo also says organisational structure is a particular weakness as he claims they are still "not integrated."

In addition to the weaknesses identified by Mr Sucahyo, many experts point to an educational deficit. "Capacity building," says Mr Nugraha when asked about a particular weakness, "because the weakest link is people and we lack awareness." Likewise, Ms Radianti says "awareness for people" is the biggest challenge and calls on the government to better prepare society for cyber security.

Fundamentally, says Mr Brown, effective cyber security is about regulation, awareness, and coordination. "But the topic is still relatively new and not a priority, especially in developing countries that are not as reliant on online infrastructure," he says about the challenge to convert this simple formula into action.

"But the topic is still realtively new and not a priority, especially in developing countries that are not as reliant on online infrastructure"

An internal assessment

To raise security awareness and to track progress, Indonesia has its own framework for assessing domestic information security across government agencies. The Information Security Index, also known as the KAMI index, begins with a self-assessment, followed by an evaluation of the answers and a follow-up interview by a group of assessors. In 2011-2012, 62 government organisations were evaluated across five areas of information security: governance; risk management; framework; asset management; and, technology.

The most recent internal findings appear to be similar to those identified by external observers: According to Mr Nugraha, in 2011-2012, the highest scores were in the technology and asset management areas while the lowest scores, and hence the greatest weaknesses, were in risk management followed by governance.

Recommendations

To reap the full benefits of the information society as the country develops, Indonesian executives and policy-makers should consider the lessons learned elsewhere and develop appropriate measures to meet the cyber security challenge. Although it is acknowledged that some of this work is already under way, findings throughout this report indicate that the following measures can be enhanced further.

1: Make cyber security a priority, at home and abroad

Indonesia has identified the importance of ICT to its socio-economic well-being. Given its increased reliance and rising user base, now is also the time to recognise the tie between ICT dependency and cyber security. This means making cyber security a priority both domestically but also internationally.

[66] The Jakarta Post:
http://www.thejakartapost.com/news/2011/11/19/online-threat-govt-told-strengthen-cyber-security.html

At home, Indonesia currently lacks a formal cyber security strategy. Abroad, Mr Simanjuntak is looking for a platform in which to work with the global community: “For cyber crime, there is a good international framework; we are not there yet for cyber security,” he says. “Cyber security is by nature a global matter, so when we think about addressing the preparation gap it’s no use trying to address it unilaterally in a corner,” agrees Ms Kroes. “It’s necessary to coordinate wherever possible, at the highest levels possible.”

2: Assess what needs to be done

Once cyber security has been made a top policy priority, the process of developing a domestic and international risk assessment begins. “It may sound simple, but the first step is to understand what you want to protect, an understanding of the threat, and the potential business impact or what the impact is on your national interest,” says Marco Obiso, Cybersecurity Coordinator at the ITU.

In Indonesia, this process should include a formal definition of critical infrastructures, which it currently lacks.[67] In addition, suggests Mr Lumanto, the government should ask such industries to develop certain security standards and incident handling capabilities.

3: Strengthen the regulatory environment

After identifying key objectives, regulatory measures should be taken to match them. The current legislation is frequently cited as Indonesia’s most glaring weakness in meeting the cyber security challenge by interviewees and public sources alike. Part of the problem stems from the fact that it deals primarily with cyber crime, which is a subset of broader cyber security issues.

It is also important to note that a stronger regulatory environment does not necessarily mean an end to self-regulation or additional burden to individual organisations: the rules simply need to be clarified for the benefit of everyone. “Strong regulation is definitely a good thing,” says Mr Keller at XL as he calls for a particular focus in enhancing privacy laws in the country. With a global viewpoint, Mr Mui says deterrence is also an essential step in protecting a country from hackers. “In this regard, strong regulations are an important part of a strong defence,” he says.

4: Enhance awareness and improve skills

Equipped with the necessary mandates, significant hurdles in implementation remain due to what many call the biggest challenge: people. In Indonesia, knowledge is low despite attempts to raise it and many people, like Mr Watuliu, are calling for an improvement in both public awareness and public education. It is not a challenge unique to Indonesia but more innovation is needed to improve awareness, particularly as governments often struggle to enhance it on their own.

[67] In the US, for example, there are 18 designated critical infrastructures, which are: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defence industrial base; emergency services; energy; government facilities; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; transportation systems; and water:
http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Indonesia also suffers from a technical talent shortage. For example, Mr Guntur and Mr Watuliu, representing the private and public sectors, both agree that there is a lack of cyber security skills when it comes to digital forensics and cyber crime. In addition to the two existing training centers belonging to KOMINFO in Ciputat and in Cikarang, the new cyber security initiative at Bandung should help, as does the efforts by Mr Heru who aims to train and certify 200 people this year, despite a cost of about 20m Rupiah or about USD 2,000 per person. However, although such efforts are welcome, they remain limited and better coordination and more resources appear needed to secure a digital workforce.

5: Coordinate a stronger multi-stakeholder approach

Although PPPs may not work optimally, the private sector and civil society continue to play vital roles in cyber security, as does all individual users. Improving education and awareness is only one area which exemplifies that there must be a role for all stakeholders. Mr Keller says basic security starts with the education system and that there are important roles for both government, particularly in terms of legislation, as well as the private sector. “Industry needs to get together and create advisory boards,” he says. “We are not competing on security but it is in our own interest to do so.” Indonesia appears to have done about as well (or as poorly, depending on your view) as anyone else in this area.

The recognition of such approach, however, is only the first step. “One thing that is still missing is the leadership from government,” says Mr Rahardjo. “There are too many uncoordinated initiatives.” With numerous programmes in place, including multiple CERTs/CSIRTs, the problem is that they are “fragmented,” according to a number of interviewees. Yet, cyber security requires a well-coordinated approach. “One authority should be in charge of cyber security,” agrees Mr Obiso. In Indonesia, KOMINFO is the lead Ministry for civilian cyber security but there is no well-defined central coordinating structure that encompasses all stakeholders. To avoid future turf battles, such policy should be enacted or the responsibilities of KOMINFO should be elevated.

6: What gets measured gets done: develop a cyber security strategy

In closing, we return to the first recommendation: to make cyber security a priority, Indonesia needs to develop a strategy that recognises the socio-economic benefits and potential consequences of ICTs. Such a strategy should be comprehensive and set clear targets and objectives from which progress can be tracked, to the benefit of Indonesia and the world.“The urgency is not there yet,” says Mr Simanjuntak, “and ignorance of cyber defence is a threat in itself.”

About DAKA advisory
We provide strategic advisory and research services and work with a broad range of clients from the private and public sectors to improve their decision-making and effectiveness. Our cyber practice focuses on cyber security, e-government, measurement of the information society and related topics primarily for the public sector.

For more information, please contact Kim Andreasson, Managing Director, at:
kim@DAKAadvisory.com

Visit us at:
www.DAKAadvisory.com

Disclaimer
Our aim is always to provide accurate information from reliable sources. However, neither DAKA advisory, nor the sponsor, can accept any responsibility or liability for the data, information or statements contained within this report.