POLICY BRIEF

Cyber security policy towards Indonesia

How to manage the growing risk

September 2017

Kara Kelly, Sita Khiani, Lachlan McGrath,
Damon Vavros and Miriam Asar

YOUNG AUSTRALIANS in
INTERNATIONAL AFFAIRS

Cyber security policy towards Indonesia: How to manage the growing risk

By Kara Kelly, Sita Khiani, Lachlan McGrath, Damon Vavros and Miriam Asar

Image credit: Mia Salim, DFAT, Creative Commons

Executive Summary

Australia must take a leading role in mitigating the growing cybersecurity threat in Southeast Asia. Indonesia is an important partner to engage to this end, due to our existing military, policing and diplomatic relationships. But also because Indonesia is a hotbed for malicious cyber activity.

Through two key recommendations with low financial and political costs, the Australian and Indonesian governments can develop their joint cybersecurity capacities in a short timeframe and respond to this growing threat.

First, this brief recommends that an Australian-Indonesian cybersecurity agency and a permanent joint task force operation be established as a matter of priority. This agency would provide an important link to the Australian Cyber Security Centre. This targeted approach would shift the focus away from broad security and toward specific cybersecurity issues.

This strategy would act as a both a deterrent for cyber criminals and also assist Indonesia in developing its internal capacity. By increasing Indonesia's ability to combat cybercrime, Australian and the region will benefit.

Second, this brief recommends that Australia and Indonesia work collaboratively to develop a legislative framework for Indonesia that aligns with Australia's current legislative stance on cybercrime.

These recommendations, if implemented successfully, could also provide a framework for collaboration with other states in the region. They would establish practices and precedents that could be easily transferred, helping to mitigate this threat area and establishing Australia as a regional leader in cybersecurity.

Background

Indonesia is highly vulnerable to cybercrime. KPMG has estimated that from 2013 to 2016, Indonesia experienced 36.6 million cyber-attacks. It also noted that between 2015 and 2016, cyberfraud in Indonesia increased by 1266%. The country also seems to be a source of cybercrime. According to Indonesia's National Cyber Agency, the country was responsible for 38% of the world's malicious internet traffic in 2016. The agency attributes this to Indonesia's security naivety and vulnerability to exploitation.

Statistics from 2015 show that of Indonesia's 256 million people, 88 million have internet access and 74 million are active on social media. These figures demonstrate how connected Indonesians are, but they also highlight large vulnerabilities and threats.

Indonesia has developed legislation to combat and detect cybercrime, but it has not created the appropriate infrastructure. For example, there is a lack of appropriate coordination between agencies, and cybercrime strategies are often narrow rather than holistic.

Australia and Indonesia already cooperate at some level on cybercrime. In a joint statement released by the Indonesian and Australian governments in February 2017, both countries expressed a desire to engage one another to combat cyber threats. They have also agreed to establish a joint cybercrime office for gathering intelligence. In addition, the Australian Transaction Reports and Analysis Centre (AUSTRAC) and its Indonesian counterpart, the Financial Transaction Reports and Analysis Centre (PPATK), announced in February 2017 that they would combine forces to launch a new project to tackle cyber fraud and terrorism financing.

Delay in implementing cybersecurity measures are costly. KPMG has found that a lack of action could cost Indonesia US$3 trillion by 2020. Such a massive cost would undoubtedly affect Australia, and highlights the need for closer cooperation between Australia and Indonesia on cyber issues.

The Challenge

Australia must re-evaluate its relationship with Indonesia as a strategic partner in cybersecurity for three key reasons. First, Australian government policy has historically lacked direction in this area and requires genuine clarification. Second, there has been a marked proliferation of threats in the cyber landscape. Third, Indonesia does not currently

have a strong cybersecurity regulatory framework that can properly deter cyber criminals from attacking nation states, individuals and other entities.

Australia's lack of strategic direction is evident through the timeline of government initiatives in cybersecurity. The Australia Cyber Security Centre opened in early 2014, and has the self-described function of 'lead[ing] the Australian government's operational response to cybersecurity incidents'. Published in 2016, the government's Cyber Security Strategy was the first of its kind in Australia. The Australian Government is currently formulating an updated strategy. However, a lot of work needs to be done in order to strengthen and cement Australia's role as a regional leader in cybersecurity.

The expansion of the cybersecurity landscape requires Australia to urgently clarify its strategic direction with Indonesia. This has been particularly pronounced in several recent cases in which Indonesia faced difficulty with cybersecurity coordination and crime prevention, as described in the previous section.

The threat environment has grown as a result of a combination of factors, each of which needs to be addressed more comprehensively by states. Cyber criminals are constantly innovating and are able to quickly exploit emerging technologies. The growth of the *Internet of Things* (IoT) has led to an increased number of seemingly innocuous internet-connected objects being exploited, such as the Cloud Pets Teddy Bear which failed to secure two million message recordings and 800,000 customer emails and passwords.

Threat proliferation is also a result of increased data flows and collections. Businesses are gathering customer data in growing amounts, which is problematic as specific companies, products and services are becoming indispensable to the average consumer. Moreover, the digitisation of data poses a significant problem. Biometric data digitisation, if compromised, would create a massive privacy violation and have implications for fraud. Unlike passwords and PIN codes, biometrics cannot be changed.

Further to this, states and their relevant policing bodies are responsible for identifying increases in cybersecurity threats much less prosecute cyber criminals. In retrospect, a large proportion of cybercrimes remain unsolved, allowing perpetrators to learn from their mistakes and undertake better preparation for their next attack.

Recommendations

Below are two recommendations that provide both the Australian and Indonesian governments with feasible and long-term solutions to address the burgeoning cyber security risk. These recommendations are designed to work in conjunction to build a robust relationship that can effectively reduce cybercrime in Indonesia and against Australia.

1. Leverage existing Australian resources in Indonesia

The Australian and Indonesian governments have a historical partnership of defence in the Asia-Pacific. In a changing world, however, attacks are no longer limited by physical means: they target countries and their citizens through cyberspace. The Australian Federal Police (AFP) has established the Australian Cyber Security Centre (ACSC), which has been operating since 2014 for the purpose of combating cyber-attacks. Indonesia's Coordinating Minister for Political, Legal and Security Affairs stated earlier this year that Indonesia is in the process of creating a dedicated cybersecurity agency. This agency will operate parallel to the ACSC. However, there is a possibility to broaden collaboration and cooperation.

Since the Bali Bombings in 2002, the AFP has maintained a physical presence in Indonesia for counter-terrorism purposes. At the peak of operations, approximately 500 AFP members were based in Indonesia. Currently only 23 AFP remain in Indonesia for support on counter-terrorism. The decline in AFP presence is due to the reduction of the terrorism threat in Indonesia. That cooperation can provide a framework for joint operations between the Australian and Indonesian government on cyber threats. By using this framework, the two countries can develop a mutual partnership against cybercrime. This would give Indonesia access to specific personnel with the required technical experience to assist the Indonesian government in the detection and reduction of cybercrime.

By leveraging these existing resources, relationships and the commitment made by the Australian and Indonesian governments, these recommendations can be implemented at lower financial costs and in less time, therefore reducing the likelihood of cyber-attacks originating from Indonesia against Australia.

2. Legislative framework

In a joint statement between the Australian and Indonesian governments published in February 2017, cyber security was highlighted as a motivation for developing an Australia-Indonesia Cyber Policy Dialogue. This recommendation positions such a dialogue to focus on developing a legislative and policy framework to advance this objective.

This framework would be rolled out in three phases:

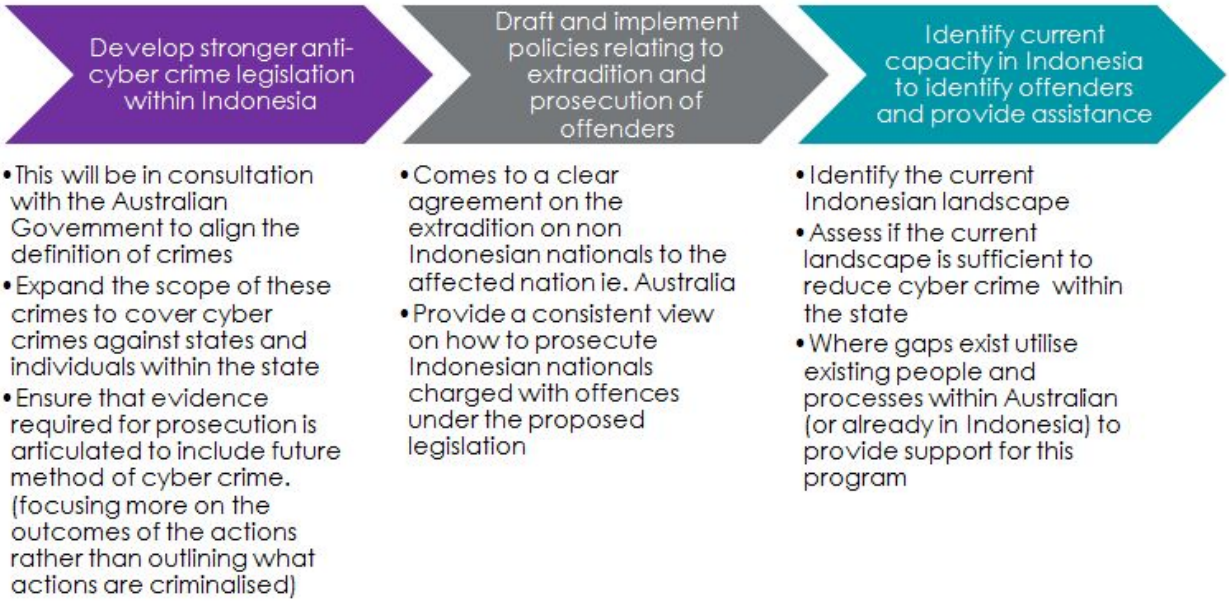

Image: Identifies a proposed roll-out of the recommended legislative framework.

1. Provide guidance and assistance to the Indonesian government to develop anti-cybercrime legislation relating to actions committed within Indonesia, against Australia (public and private) and against Australian citizens.

2. Develop clear and detailed policies and guidelines outlining methods of cooperation between the Australian and Indonesian governments on either extradition and/or prosecution of people charged under this legislation. Enforceable legislation would mitigate the risk that Australia or Indonesia are unable to take effective action against those who perpetrate crimes against Australia and its citizens. This risk was recently evident in the US when the US government was unable to extradite a Russian citizen who was indicted for a series of cybercrimes.

3. Identify the current Indonesian cybersecurity and law enforcement landscape, including capacity of personnel, effectiveness of processes and quality of available technology. Where gaps are identified, existing personnel and processes within Australian (or already in Indonesia) should be utilised to provide support for this program.

As the scope of this recommendation indicates, there are inherent weaknesses associated with cybercrime policies. These challenges are compounded by the complex and ongoing cooperation required to achieve a sustainable and effective framework. Below are a set of challenges in this recommendation, as well as the associated strengths that would arise should this framework be successfully implemented.

Weaknesses within the proposed legislative framework:

- The potentially arduous costs of developing and implementing new legislation.
- The risks around aligning this legislation with Australia's current political strategy, and maintaining the legislation should there be any shifts in Indonesia's existing strategic framework.
- The inherent risk within cybercrime around the issue of attribution and identifying the perpetrator.
- Indonesia does not currently have strong cybercrime legislation outside of its adoption of the Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions.

Strengths within the proposed legislative framework:

- Indonesia can leverage existing Australian legislation to reduce time and effort costs.
- By providing this framework, Australian businesses might be less hesitant to enter the Indonesian market. A legislative deterrence to cybercrime with an enforcement mechanism would provide an incentive for businesses looking to build offshore capabilities in more cost-effective countries, such as Indonesia, with the confidence that their information will be legally protected.
- Developing a strong legislative base would provide both countries with a framework for managing cyber relations with third countries where cyber criminals are also active.

Given the complex nature of cybercrime, an alternative to this framework is the establishment of a Memorandum of Understanding (MoU). This would provide an avenue to extradite cyber criminals to Australia who are charged with committing crimes against Australia or Australians. An MoU would not have the strength of enforceable legislation, but could be used to begin cooperation between the countries until a future agreement over a framework is negotiated.

Conclusion

The relationship between Australia and Indonesia has enormous potential that could see a rapid increase in the securitisation of digital borders. Action is required to ensure the developing theatre of cyberspace is protected with the same seriousness as national and private assets in physical space.

For any new security structure between Australia and Indonesia to function effectively, it must engage stakeholders and peak bodies that are profoundly aware of the security implications for countries, citizens and relationships. Further to this, it requires a careful appraisal of the opportunities to strengthen our position within Australia and across the globe through a judicious choice of national and foreign policy priorities.

The expansion of the cybersecurity landscape will require Australia to review the aforementioned challenges as set out in the key recommendations provided. These recommendations aim to leverage existing assets and networks between Australia and Indonesia to respond to existing and developing threats with increased capabilities. Finally, closer coordination on policy production and legislative responses will further empower the two authorities while engendering a landscape that inhibits cybercrime.

Bibliography

Department of Prime Minister and Cabinet, 'ADM—Cyber Security Summit', 2017, <https://www.dpmc.gov.au/sites/default/files/files/pmc/FAS_CPI_ADM_CSS_speech_170615.pdf>, [accessed 21 March 2017].

Anjum, Z, 'Cyber attacks an increasing concern for Asean countries', *ComputerWeekly.com*, 2015, <http://www.computerweekly.com/news/4500260196/Cyber-attacks-an-increasing-concern-for-Asean-countries>, [accessed 21 March 2017].

Attorney-General, Senator The Hon George Brandis QC and Minister For Justice
Minister Assisting The Prime Minister for Counter-Terrorism, The Hon Michael Keenan MP 'Joint Communiqué: 2017 Australia-Indonesia Ministerial Council on Law and Security', 2017, <https://www.attorneygeneral.gov.au/Mediareleases/Pages/2017/FirstQuarter/Communique-2017-Australia-Indonesia-Ministerial-Council-on-Law-and-Security.aspx>, [accessed 21 March 2017].

Austrac, 'Regional Risk Assessment on Terrorism Financing 2016: South-East Asia & Australia', 2016, <http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf>, [accessed 21 March 2017].

Australian Cyber Security Centre, 'Frequently-Asked Questions', 2014, <https://www.acsc.gov.au/faqs.html>, [accessed 16 March 2017]

Australian Federal Police, 'The Australian Cyber Security Centre - "Partnering for a Cyber Secure Australia"', 2017, <https://www.afp.gov.au/what-we-do/crime-types/cybercrime/australian-cyber-security-centre-partnering-cyber-secure-australia>, [accessed 21 March 2017]

Australian Federal Police, 'Countering Terrorism' <https://www.afp.gov.au/sites/default/files/PDF/countering-terrorism.pdf>, [accessed 10 June 2017].

Baka, P, 'Southeast Asia Still Has Weak Information Security Against Cyber Threats', *The Diplomat*, 2017, <http://thediplomat.com/2016/10/southeast-asia-still-has-weak-information-security-against-cyber-threats>, [accessed 21 March 2017].

Cooper, L, 'Millions of Private Messages Between Parents and Kids Hacked in Cloud Pets Security Breach', *The Huffington Post*, 2017, <http://www.huffingtonpost.com.au/2017/02/28/millions-of-private-messages-between-parents-and-kids-hacked-in/>, [accessed 21 March 2017].

Coyne, J, ‘The AFP needs to co-operate with Indonesia on fighting terror’, *The Australian*, 2015, <http://www.theaustralian.com.au/opinion/the-afp-needs-to-cooperate-with-indonesia-on-fighting-terror/news-story/0f85e006bd0c5f1bad51e5e3322d757d >, [accessed 21 March 2017].

Fireeye, ‘Fireeye Threat Intelligence—Southeast Asia: An Evolving Cyber Threat Landscape’, 2015, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf>, [accessed 21 March 2017].

France-Presse, A, ‘Dutch will count all election ballots by hand to thwart hacking’, *The Guardian*, 2017, <https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking>, [accessed 21 March 2017].

Hoang, L, ‘Southeast Asia Cybersecurity Risks have Global Effect’, *Bloomberg Law: Privacy & Data Security*, 2017, <https://www.bna.com/southeast-asia-cybersecurity-n73014449868/>, [accessed 21 March 2017].

Kokoshin, A, *Reflections on Russia's past, present and future*. 1st ed., Cambridge, Mass., Strengthening Democratic Institutions Project, John F. Kennedy School of Government, Harvard University, 1997.

KPMG, ‘Cyber Risks in Emerging Markets’, 2015, <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/SG-Advisory-CS-Cyber-Risks-in-Emerging-Markets.pdf>, [accessed 21 March 2017].

News Desk, ‘Cyber Attacks in Indonesia Rising at Alarming Rate: Officials’, *The Jakarta Post*, 2016, <http://www.thejakartapost.com/news/2016/06/03/cyberattacks-in-indonesia-rising-at-alarming-rate-officials.html>,
[accessed 21 March 2017].

Parameswaran, P, ‘A New Cyber Agency for Indonesia?’, *The Diplomat*, 2017, <http://thediplomat.com/2017/01/a-new-cyber-agency-for-indonesia>, [accessed 21 March 2017].

Parameswaran, P, ‘Does Indonesia Need a New Cyber Agency?’, *The Diplomat,* 2016, <http://thediplomat.com/2016/09/does-indonesia-need-a-new-cyber-agency/>, [accessed 21 March 2017].

Prime Minister of Australia the Hon Malcolm Turnbull, ‘Joint Statement Between the Government of Australia and the Government of the Republic of Indonesia’, Department of Prime Minister and Cabinet, 2017,
<https://www.pm.gov.au/media/2017-02-26/joint-statement-between-government-australia-and-government-republic-indonesia>, [accessed 21 March 2017].

The Republic of Indonesia, Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions enforced April 21, 2008.

Rustici, K, ‘Indonesia’s Cybersecurity: An Opportunity for Deeper Cooperation’, *CSIS*, 2013, <https://www.csis.org/analysis/indonesia%E2%80%99s-cybersecurity-opportunity-deeper-cooperation>, [accessed 5 September 2017].

Trimmer, A, ‘Identity Management and the Application of Biometric Technology’, *Computers & Law*, December, 2005, pp. 13-15.

United States Government, Department of Justice, ‘U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts’, 2017, <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>, [accessed 21 March 2017].

Yosephine, L, ‘Indonesia, Australia strengthen cyber-security ties’, *The Jakarta Post*, 2017, <http://www.thejakartapost.com/seasia/2017/02/03/indonesia-australia-strengthen-cyber-security-ties.html>, [accessed 21 March 2017].