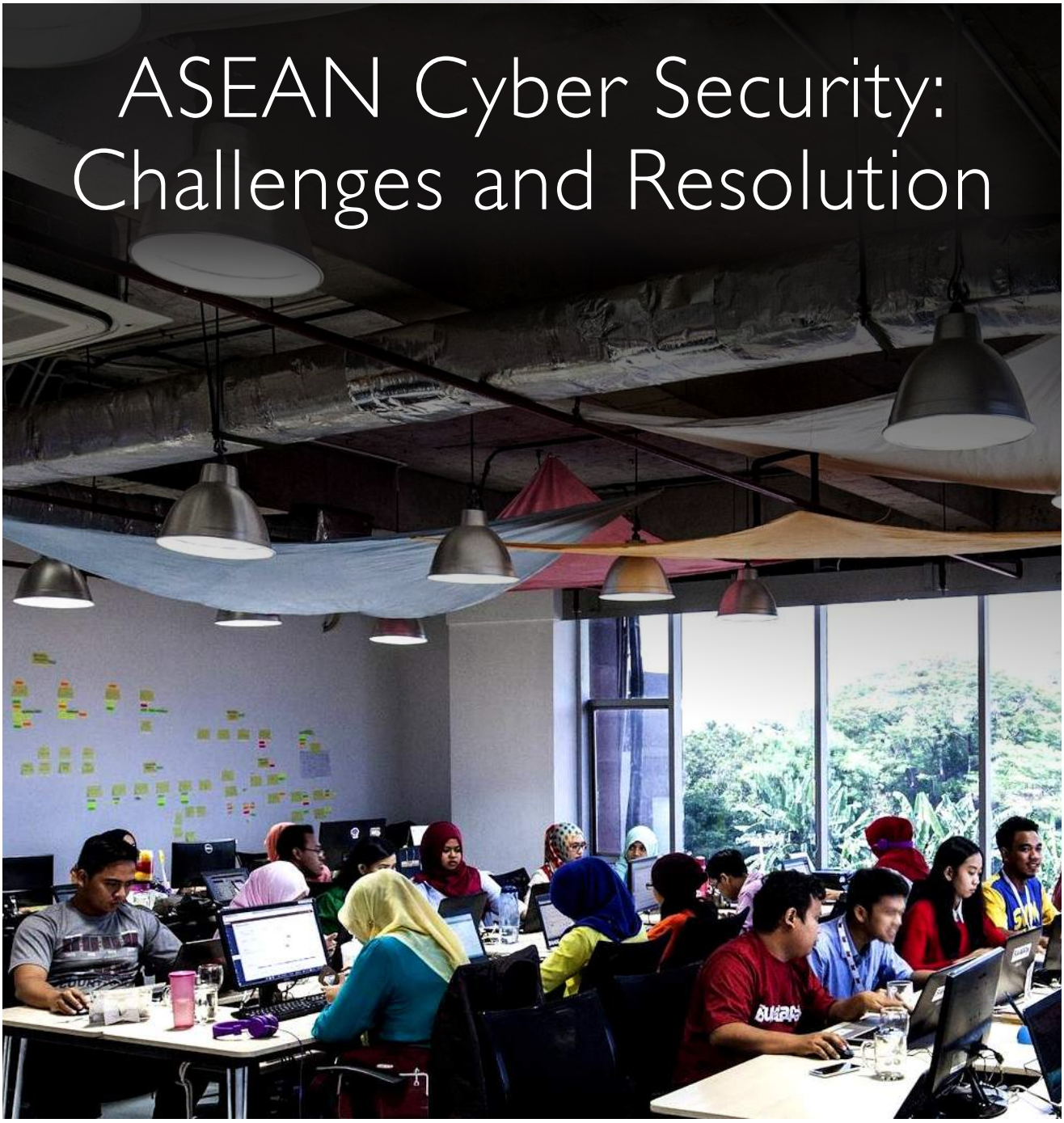
# ASEAN Cyber Security: Challenges and Resolution



**Bukalapak Office**
*Source: stackoverflow.com*

**Brian Kumara** *is an independent researcher*

Offering smartphones to televisions and even virtual reality (VR), technology has become a central aspect of our lives. By March 2017, there were around 321,913,948 internet users in the Association of the Southeast Asian Nations (ASEAN).[1] While the ratio of internet usage is lower in Asia than in Europe or North America, the influence of technology and the digital world in ASEAN is very significant. To illustrate, a research published by Temasek Holdings, Singapore's national wealth fund, and Google revealed that the projected worth of ASEAN's digital economy would be around USD 200 billion each year by 2025, showing that the digital world is full of potential for ASEAN members.[2] For example, Indonesia is tipped to be the region's biggest digital market, with a growth in user by 19% per annum and e-commerce worth USD81 billion by 2025.[3] The emergence of online-based transportation services such as Uber, Grab, and Gojek has boosted Indonesia's digital economy, making it the biggest in ASEAN and worth USD800 million in 2015.[4]

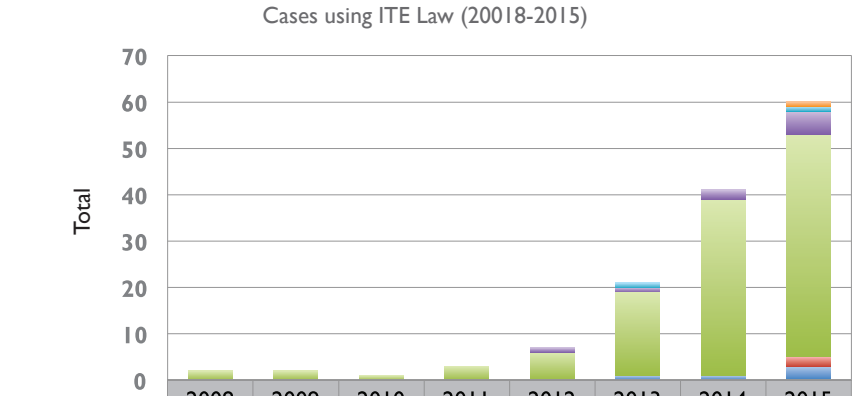
However, the rise of the digital economy and technology in general has presented some security issues around the world. For instance, the United Kingdom's National Health Service (NHS), Home Box Office (HBO), and Sony Entertainment have been hit by cyber attacks that stole sensitive information and demanded ransom from these entities. [5] [6] In Malaysia, around USD 900 million was lost between 2007-2012 due to cybercrimes whilst Indonesia lost USD2.7 billion per annum.[7] Hence, the threat posed by cyber crimes harms ASEAN's goal of economic prosperity and security. However, arguably little is being done to address such digital issues that ASEAN currently faces. While, some government ministers have called for a collectivized cybersecurity scheme, no policies have been introduced yet.[8] While an ASEAN Chief of Information Officer Association (ACIOA) exists, its scope is very limited.[9] Hence, this article will explore what are the current major digital threats that ASEAN members face, alongside the potential solutions that members may use to curb digital threats.

With regards to strengthening cyber security, it is important to note that there very few international treaty that addresses cybercrime. The 2001 Budapest Convention on Cybercrime aimed to harmonize local laws pertaining to cybercrime by setting up a proper procedural legal powers for offences committed through a computer and evidences in electronic forms. However, as of 2017, no ASEAN member has ratified the treaty.[10] In October 2016, the ASEAN Ministerial Conference on Cybersecurity (AMCC) convened for the first time, and members called for "closer cybersecurity cooperation among ASEAN countries, stronger coordination of regional cybersecurity capacity building initiatives".[11] However, no concrete policies were suggested and as of August 2017, there has been no further announcement from the AMCC. While a step in the right direction, more needs to be done by members to ensure digital safety.

Examining ASEAN members individually, it seems that only Singapore has a comprehensive cyber policy that is already in place. This is outlined in their "Four Pillars" strategy.[12] The first pillar focuses on building a strong infrastructure for the digital economy from online banking to e-government. This was done through a cooperation between the private and public sector to raise security standards and also by raising the security standards by which private firms operate. The private sector is also responsible for alerting the government on cyber crimes and conducting exercises to test for weaknesses in the system. The second pillar revolves around the idea of a "safe cyber space". Again, this is done through the collaboration between the private and public sector. The third pillar aims on developing Singapore's cybersecurity workforce. This is done by offering a Cyber Security Associates and Technologists (CSAT) programme that provides a six-month training to IT professionals with three years of experience. The fourth pillar, recently announced, focuses on international cooperation through agreements with the United States, United Kingdom, France, the Netherlands, and India.

By contrast, the cyber policy of other ASEAN members are not as sophisticated. For instance, the Philippines has announced their National Cybersecurity Plan for 2022.[13] However, it only mentions general statements such as "cybersecurity educated society" and "implementing cyber resiliency" without plans to achieve these goals.[14] Indonesia is a member state tipped with the second highest malware threat, coming only behind Pakistan in the world. [15] Compared to Malaysia, which has the Computer Crime Act (1997), Digital Signature Act (1997), Telemedicine Act Multimedia Act (1998), Payment System Act (2003) and a Personal Data Act (2010), Indonesia only has the Telecommunication Law No. 36 (1999) and the controversial Information and Transaction Electronic Law (ITE) (2008).[16] [17] Worse still, the ITE is used mostly for defamation cases and the country focuses its IT efforts on blocking pornographic sites instead of increasing its cyber security standards. The following chart highlights the use of the ITE:[18]

Indonesia also has not approved a nation-wide security framework.[19] Despite the




| | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|---|
| Artc31 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Artc29 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| Artc28(2) | 0 | 0 | 0 | 0 | 1 | 1 | 2 | 5 |
| Artc27(3) | 2 | 2 | 1 | 3 | 6 | 18 | 38 | 48 |
| Artc27(1) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| Legal Notice | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 3 |

*Source: Safenet (2016)*

legal weaknesses, Indonesia has a strong technical capacity. The nation is a member of APCERT FIRST (Asia Pacific Computer Emergency. Response Team - Forum for Incident Response and Security Team), also founding member of OIC-CERT (Organisation of The Islamic Cooperation – Computer Emergency Response Teams). Yet, involving the non-public sector seems to be difficult, and many have noted that it is based on personal relationship as opposed to organizational cooperation.[20] Consequently these groups tend to work and establish their own framework different from the government.[21] This leads to a wide disparity between security standard in the private and public sector.

Another member of ASEAN that lacks cyber security policies is Cambodia. An article concluded that eight in ten computers did not have security measures as they used non-genuine systems.[22] Other nations like Myanmar do not have a cyber policy and instead rely on an emergency team (MMCERT), meaning that they only have a containment policy but not a prevention policy.[23] Thailand does not have a specific law regarding data protection but does have the Computer Crime Act (CCA) to prevent fraud and identity theft.[24] Worse still is Vietnam. The country is prone to hacks due to the lack of cyber enforcement, with hackers attacking one of its airports recently. On the other hand, the government is reluctant to allow encryption as it prevents the monitoring of citizens' activities.[25] As a result, the cyber security capacities and regulations differ greatly from one ASEAN member to another.

On a collective basis, ASEAN members are involved in the ACIOA. While this is a step in the right direction by offering initiatives such as business-government cooperation and a Chief of Information Officer (CIO) academy training, their activities are limited to CIO. An expanded training program as seen in Singapore's current cyber policy would be hugely beneficial in creating a cybersecurity workforce in ASEAN members. However, there are some limitations. At the moment, only Singapore seems to offer a comprehensive training scheme. Yet, it would be irresponsible to place the pressure on Singapore alone for training considering the logistical consequences such as manpower and living space. Secondly, funding may be an issue. The lack of government funding will deter people from the lower income spectrum to train in cyber security due to travel and living costs and such. Due to the difference in the availability of government funds, ASEAN members should look into possible cooperations with outside countries, such as its Dialogue Partners, and find alternative means of financing these individuals through loans.

Currently, Japan is working with ASEAN and has released a CIIP (a national procedure for cyber security).[26] The new strategies in this policy should be integrated into an ASEAN wide digital policy after taking considering the current conditions of its members. While Japan and ASEAN has launched a collaborative program of study, more intra-cooperation would be beneficial to the collective cyber security ASEAN needs. A recent research by Accenture published the following digital challenges for ASEAN:[27]

1. Weak business case for building out broadband
2. Regulations inhibiting innovation in mobile financial services and e-commerce
3. Low consumer awareness and trust hindering the uptake of digital services
4. No single digital market
5. Limited supply of local content, primarily due to a weak local digital ecosystem

While not necessarily specific on cyber security, there are some lessons from the analysis above. For instance, the lack of businesses building better broadband shows a lack of investment in infrastructure. A government scheme can help persuade investors to improve the digital infrastructure, and the option of lower tax should be considered. While offering better broadband connectivity to consumers, companies have a chance to implement cyber security measures such as security-by-design and computer intrusion detection. A weak digital ecosystem does not necessarily apply to all ASEAN members (Singapore comes into mind), but programmes to raise digital awareness and aptitude can go a long way to avoid scams and hacks for all members. Hence the current solution seems to be increasing government expenditure on technology related activities while enticing businesses to build a better system.

Another issue regarding cyber security in ASEAN is the workforce retention. While it is necessary to train capable cyber security employees and form policies to protect the digital world, it would be for naught if employees are quick to move to other countries or other industries. Just as there are different level of cyber security policies and capabilities amongst ASEAN members, there are different retention rates for skilled workforce. For instance, Singapore does not face a labour retention crisis to the point where the IMF signals worry over falling numbers of foreign workers.[28] On the other hand, countries such as Indonesia face a shortage of skilled engineers.[29] While the labour situation varies, it is clear that without a stable and sizeable technologically-skilled workforce, it is impossible to protect a nation's cyber security, let alone for ASEAN. Hence, the development of cyber securities needs to come with the capacity for governments to persuade local and international talents to stay in their countries, which comes from a self-analysis for each member as they have different situations.

As a short term solution, cyber related events such as hackathon for ASEAN members can be hugely beneficial to quickly identify flaws in the system. However, this should not be regarded as the ideal approach. Instead of having outside parties identify the flaws, ASEAN members should focus on internal development and constant innovation to avoid cyber attacks. Since that is not possible in the short term, hackathons should be a remedy until a competent cyber security workforce is in place to identify flaws and improve security standards. The long term goal of ASEAN members in terms of tackling cybercrime should be to form an organization similar to the Joint Cybercrime Action Taskforce (J-CAT) in the European Union. At the moment, J-CAT has initiatives to:[30]

1. Select the most relevant proposals;
2. Share, collect and enrich data on the cases in question;
3. Develop an action plan, which is led by the country that submitted the selected proposal;
4. Go through all the necessary steps to ensure the case is ready to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification the required resources and the allocation of responsibilities.

Unlike the European Union, ASEAN does not have a European Court of Justice. This clearly causes issues for legal aspects. However, given the current calls for harmonizing cyber securities amongst members, the legal aspects an obstacle that members should be able to overcome quite easily through talks .

Another aspect is collaboration on cyber security should come through the ASEAN Defence Industry Collaboration (ADIC).

Members should expand from selling defence equipment and focus on digital protection equipment and services. ADIC members do not currently buy substantial amounts from other ADIC members, instead opting to source their current defence equipment from outside nations such as the United States and the United Kingdom.[31] Should Singapore decide to offer technical services and training, in time, other members may see a rise in cyber security standards by hiring experts from ASEAN and essentially form an interconnected cyber security workforce and start trading internally.

In conclusion, the disparity of cyber security standards between members of ASEAN varies greatly, creating different levels of challenges from one member to another. On the one hand is Singapore, with robust cyber security from the "Four Pillars" strategy that focuses on private-public cooperation on identifying weaknesses, preventing unsafe online content, training new workers, and international agreements. On the other hand are countries like Thailand, Cambodia and Vietnam, whose lack of cyber security policy and standards have made it an appealing target for hackers. To counteract the disparity, ASEAN members can look forward to expanding their ACIOA to lower ranked employees for cybersecurity education. Members should also act quickly to harmonize ASEAN digital standards and ensure that an organization similar to J-CAT is created. Yet, they must consider the more subtle factors to achieve these proposals. For instance, ASEAN members need to find a way to retain their workforce and ensure that after a certain period of time, the training responsibility is not just concentrated in Singapore. Additionally, short term events such as hackathon can help identify talents, which can then be retained, while also identify system flaws. In the long run, ASEAN members should aim to have a continually innovative cybersecurity industry to prevent hacking and an ADIC that can supply cyber security services to less sophisticated members. Returning to its economic prospects, countries like Indonesia can look forward to enjoying a $85 billion USD digital market if its investors are confident that the cyber security standards and policies can protect confidential information and prevent frauds.[32] Looking at the current situation, it seems highly likely that members can progress rapidly so long as cooperation and commitment is maintained for the next few years.

## Endnotes


1 "Internet Usage in Asia." *Asia Internet Usage Stats Facebook and Population Statistics*, Miniwatts Marketing Group , <www.internetworldstats.com/stats3.htm>

2 Russell, Jon. "Report: Southeast Asia's Internet Economy to Grow to $200B by 2025." *TechCrunch*, TechCrunch, 24 May 2016, <www.techcrunch.com/2016/05/24/report-southeast-asias-internet-economy-to-grow-to-200b-by-2025/>

3 "Indonesia to Become The ASEAN's Biggest Digital Economy Country." *Invest in Indonesia*, Indonesia Investment Coordinating Board, <www.bkpm.go.id/en/article-investment/readmore/indonesia-to-become-the-aseans-biggest-digital-economy-country>

4 Ibid.

5 "NHS under cyber attack." *Financial Times*, www.ft.com/content/ced6dd82-6709-11e7-9a66-93fb352ba1fe.

6 Flynn, Conner. "HBO Hack Feared To Be Larger Than Sony Hack." *Geeky Gadgets*, 6 Aug. 2017, <www.geeky-gadgets.com/hbo-hack-feared-to-be-larger-than-sony-hack-07-08-2017/>

7 Lee, Stacia. "ASEAN Cybersecurity Profile: Finding a Path to a Resilient Regime." *The Henry M. Jackson School of International Studies*, 4 Apr. 2016, <https://jsis.washington.edu/news/asean-cybersecurity-profile-finding-path-resilient-regime/>

8 "ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN." *Cyber Security Agency*, 11 Oct. 2016, <www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean>

9 Kwek, Hong Sin. "Initiatives." *ACIOA*, <www.acioa.com/en/initiatives/>

10 "Budapest Convention and Related Standards." *Cybercrime*, <www.coe.int/en/web/cybercrime/the-budapest-convention>

11 "ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN." *Cyber Security Agency*, 11 Oct. 2016, <www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean>

12 Kwang, Kevin. "National Cybersecurity Strategy Aims to Make Smart Nation Safe: PM Lee." *Channel NewsAsia*, 9 June 2017, <www.channelnewsasia.com/news/singapore/national-cybersecurity-strategy-aims-to-make-smart-nation-safe-p-7743784>.

13 "National Cybersecurity Plan 2022." *Republic of the Philippines*, 10 Aug. 2017, <www.dict.gov.ph/national-cybersecurity-plan-2022/>

14 Ibid.

15 Barrett, Lauren. "Cybersecurity More than Just an IT Issue, It's a Business Issue." *Phnom Penh Post*, Post Media Co Ltd 888 Building H, 8th Floor, Phnom Penh Center Corner Sothearos & Sihanouk Blvd Sangkat Tonle Bassac120101 Phnom Penh Cambodia, 16 Dec. 2016, <www.phnompenhpost.com/supplements/cybersecurity-more-just-it-issue-its-business-issue>

16 "The National Cyber Security Policy." *Oxford Said Business School*, Ministry of Science, Technology and Innovation of Malaysia, <www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Malaysia%20Cyber%20Security%20Policy.pdf>

17 Nugraha, Leonardus K., and Dintra A. Putri. "Mapping the Cyber Policy Landscape: Indonesia." *Centre for Innovation Policy and Governance*, Global Partners Digital , Nov. 2016, <cipg.or.id/wp-content/uploads/2017/04/CIPG_Indonesia-Cyber-Policy-Mapping.pdf>

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 Barrett, Lauren. "Cybersecurity More than Just an IT Issue, It's a Business Issue." *Phnom Penh Post*, Post Media Co Ltd 888 Building H, 8th Floor, Phnom Penh Center Corner Sothearos & Sihanouk Blvd Sangkat Tonle Bassac120101 Phnom Penh Cambodia, 16 Dec. 2016, <www.phnompenhpost.com/supplements/cybersecurity-more-just-it-issue-its-business-issue>

23 "Myanmar Computer Emergency Response Team | Myanmar Computer Emergency Response Team." *Myanmar Computer Emergency Response Team | Myanmar Computer Emergency Response Team*, <www.mmcert.org.mm/>

24 Ramiah, Rajen. "Data Protection and Cybersecurity Laws in Thailand ." *Chambers and Partners*, 21 Mar. 2017, <www.chambersandpartners.com/article/1570/data-protection-and-cyber-security-law-in-thailand>

25 Gray, Michael L. "The Trouble with Vietnam's Cyber Security Law." *The Diplomat*, The Diplomat, 22 Oct. 2016, <thediplomat.com/2016/10/the-trouble-with-vietnams-cyber-security-law/>

26 Matsubara, Mihoko. "Japan's Cybersecurity Capacity-Building Support for ASEAN." *Palo Alto Networks Blog*, 25 July 2017, <researchcenter.paloaltonetworks.com/2017/07/cso-japans-cybersecurity-capacity-building-support-asean-shifting/>

27 Yan , Janet. "Digital ASEAN." *Accenture Blog*, Accenture, 10 June 2016, <www.accenture.com/sg-en/blogs/blogs-preparing-asean-digital-workforce>

28 Nation, The. "IMF Raises Eurozone Growth Forecast despite Brexit." *The Nation*, 4 Oct. 2016, <www.nationmultimedia.com/breakingnews/IMF-raises-eurozone-growth-forecast-despite-Brexit-30296910.html>

29 Cochrane, Joe. "Indonesia's Dire Need for Engineers Is Going Unmet." *The New York Times*, The New York Times, 18 Dec. 2016, <www.nytimes.com/2016/12/18/world/asia/indonesias-dire-need-for-engineers-is-going-unmet.html>

30 Joint Cybercrime Action Taskforce (J-CAT)." *Europol*, 4 Nov. 2016, <www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>

31 "Sneha Raghavan and Guy Ben-Ari (2011, September 7) Current Issues- No. 25: ASEAN Defence Industry Collaboration". *www.csis.org/ISP/DIIG/*.

32 "Indonesia to Become The ASEAN's Biggest Digital Economy Country." *Invest in Indonesia*, Indonesia Investment Coordinating Board, <www.bkpm.go.id/en/article-investment/readmore/indonesia-to-become-the-aseans-biggest-digital-economy-country>