dead channels, coming alive

an examination of emerging cyber threat activity in selected Southeast Asian nations

PREPARED FOR SIPA CAPSTONE 2017

CLIENT: FIREEYE iSIGHT

DEAD CHANNELS, COMING ALIVE

AN EXAMINATION OF EMERGING CYBER THREAT ACTIVITY IN SELECTED SOUTHEAST ASIAN NATIONS

By: Lyndon Low, Daniel Schnok, Mena Tajrishi and Jamie Welch

Advisor: Katheryn Rosen

April 2017

ACKNOWLEDGEMENTS

The Capstone team would like to thank the individuals who have made this report possible. We would like to firstly thank our SIPA faculty advisor, Katheryn Rosen, for her invaluable guidance and constant support in this endeavor. We would also like to thank the members of FireEye iSIGHT Intelligence, especially Luke McNamara, and Chris Porter, for their continuous feedback and for empowering us to work together to produce a new way of examining cyber threat activity.

We would also like to thank the many subject matter experts who dedicated their time to interviews with our team. We offer a sincere thank you to: Jason Healey – Cyber Professor at Columbia University and former White House Director for Cyber Infrastructure Protection, Franz-Stefan Gady - Senior Fellow at the East West Institute, Klée Aiken- External Relations Manager at APNIC, Francesco Brindisi - Associate Director for Economic Analysis, Forecasting, and Tax Policy at the NYC Office of Management and Budget (OMB) and Data Professor at Columbia University, Peter Roady - Columbia PhD Candidate, Jittip Mongkolnchaiaruny - Thai National and Published Cyber Expert, and Sarah Andrews - M.S. in Math Education, who provided expert help with mathematical modeling.

Lastly, we would like to thank Columbia University and specifically, Suzanne Hollmann and Saleha Awal at the School of International and Public Affairs, for organizing this capstone project and making all of this possible.

TABLE OF CONTENTS

1. Introduction

Increased anxieties surrounding cyber threat activities have forced states, institutions, business, and individuals alike to regard security in new ways. Increased connectivity, as a result of improving technology, bears new tools for statecraft and economic prosperity. However, it also introduces new understandings of vulnerability. Unfortunately for governments, businesses, and individuals, efforts to safeguard both public and private systems in order to thwart cyber threat activity cannot always ensure perfect security. The 2016 U.S. Presidential election is just one of the latest reminders of the vulnerability of the Internet's potential power and transformative impact.[1] While not all cyber threat activity aims to influence an election, it is clear that the stakes are high in an increasingly connected and interconnected world. Thus, the question begs: which countries are most likely to be future hotbeds of cyber threat activity? Recognizing the importance of this question, FireEye iSIGHT invited our team to complete the following tasks:

1. Examine various labor market drivers of cyber threat activity globally, especially the supply of hackers and offensive cyber talent.

2. Develop a methodology, if possible, for predicting growth or trends in cyber threat activity derived from data.

3. Determine, using economics/demographic data, which countries are most likely to be future hotbeds of cyber threat activity in SouthEast Asia.

Under the directive of FireEye iSIGHT Intelligence, this report examines six Southeast Asian countries: Indonesia, Malaysia, Philippines, Singapore, Thailand, and Vietnam and aims to address each of the 3 tasks posed by FireEye iSIGHT.

Intuitively, our team identified the major conditions that are necessary for cyber threat activity. We then developed a way to chart countries cyber muscularity by weighing and ranking behavior based on indicators we believe are critical to cyber threat activity. We created a method on how to weight and rank indicators allowing for a repeatable process that can be used to predict cyber threat activity globally. Finally, we analyzed each country to illustrate how it gained its cyber threat activity score and thus, ordered position amongst and against the other five countries.

This report will chart our process, present our findings, and discuss the model we created to address the questions and produce our conclusions. We have additionally provided insight and key takeaways for each country to craft an illustration of the conduct of both non-state actors and state actors in each country and their relationship to cyber tools within each respective state. In doing so, we are able to offer FireEye iSIGHT a methodology intended to assist in identifying cyber threat activity as a means to assist in their mission to provide security to their clients.

2. Foundations

To determine which country posed the greatest threat to cyber security, we had to first define the necessary conditions and environmental factors that allow for cyber threat activity. Since a model of this kind had never been developed before, to our knowledge, we sought out creative ways to approach the understanding of cyber threat activity. Ensuring our model did not unnecessarily deviate from the trove of cyber discourse, we relied on expert opinion gained from interviews with subject matter experts and numerous cyber literatures and reports. We found the *Cyber Maturity in the Southeast Asian Region* (2016) from the Australian Strategic Policy Institute report and the *Cyber Security Capability Maturity Model* (2014) report from the Global Cyber Security Capacity Centre most helpful in guiding our thinking. These first steps proved useful and enabled our team to decipher that cyber threat activity results from three specific drivers: *capability; motivation; and opportunity*.

1. *Capability*: The necessary infrastructure a state or non-state actor must possess and/or have access to in order to become a cyber-actor.

[1] Lipton, Eric.,Sanger, David.,Shane, Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S., *New York Times.* December 13, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

2. *Motivation*: The necessary conditions that prompt a state or non-state actor to take action.

3. *Opportunity*: The necessary conditions that allow states and non-state actor to take action.

Each of these three drivers may be driven by either state or non-state, or both, where levels of transference of knowledge between the two are possible and likely. Unlike the other drivers, *capability* is comprised of mostly quantitative indicators that required less subjectivity. As such, we have defined *capability* as an agnostic indicator. *Capability* is agnostic because it can be applied broadly with little subjectivity. Understanding a country's *capability*, whether in Southeast Asia, or otherwise, can be determined easily if one populates each indicator with any given country's existing technical and network system components.

Conversely, *motivations* and *opportunities* are defined as non-agnostic because the *motivations* and *opportunities* for individuals and states will differ by state, region, and situation. *Motivation* for states or non-state actors embedded in conflict may be skewed according to the definition of motivation, as motivation functions in the context within which it is embedded. This is similar for *opportunity*, as opportunities for action vary by situation dependent on state laws and enforcement. For example, in our examination of these six countries, we saw that the driving factors motivating Singapore to action were different than those that motivated Thailand.

Mindful of such country differences, our team established 60 indicators with the goal of producing a model that could capture the complex relationship each country has with cyber development and allow for comparison. Two components, *gender and investment* do not fit under any of the three main drivers. Although we could not find placements for these components in one of the three drivers, we believe the two components are too critical to our analysis to be excluded. Therefore, while they remain outside these drivers, we have none-the-less incorporated them into our research model.

All together, these factors allowed us to define the necessary conditions that allow for cyber threat activity as:

> **Cyber Threat Activity:** The activity resulting from an actor, either state or non-state, with opportunity that is both capable and motivated to carry out malicious activity.

3. Methodology

To determine which of the six countries poses the biggest threat to cyber security, we created a model to evaluate both quantitative and qualitative indicators and ascribe values based on levels of influence.

Utilizing both qualitative and quantitative indicators, our team examined the components, characteristics, and criteria necessary for cyber threat activity. We conducted interviews with journalists, former government officials, leading cyber security academics, tech gurus, and often our own colleagues. Throughout our foundational research, our team incorporated political science theory and security studies foundations while being mindful of historical, cultural, and gender nuances that may often be overlooked.

The use of both qualitative and quantitative factors was decidedly important in crafting a complete narrative. Quantitative factors alone were not comprehensive enough to create an accurate conclusion, as they do not depict the human story that exists in cyber threat activity. For a more complete picture the combination of both quantitative and qualitative factors was necessary. The combination of these factors allowed us to weave together cyber and human components and better inform our overall understanding of cyber threat activity proliferation.

The 60 indicators chosen detail the necessary components, environments, and characteristics that must be present in combinations to observe cyber threat activity. These indicators when independently analyzed tell a very limited story. The 60 indicators were categorized under the main drivers of cyber

threat activity: *capability*, *motivation* and *opportunity*. We rated these indicators low, medium, high dependent on the size of their impact on cyber threat activity. An indicator that is rated high has a large impact on whether cyber threat activity will occur. An indicator that is rated low has a smaller impact on whether cyber threat activity will occur. For example, the indicator "Access to Electricity" received a "high" categorization, as access to electricity is fundamental to conduct cyber threat activity. Conversely, the indicator "Number of ISPs" received a "low" categorization, as once the number of Internet Service Providers reaches at least one, there is enough connectivity to conduct cyber threat activity. However, to be clear, additional ISPs, while improving connectivity do not fundamentally influence or create more cyber threat activity.

In addition to categorizing indicators as low, medium or high, we felt it was necessary to determine whether an indicator has a direct or indirect impact on cyber threat activity. A direct impact was ascribed to the indicators that directly influence observable onsets cyber threat activity. For example, the indicator "Informal Economy (Black Market)" has a direct impact as the existence of such a market directly impacts how lucrative cyber threat activity can be. Conversely, the indicator "Gender Development Index" has an indirect categorization, as gender inequality is an indirect motivation that may produce grievances that in turn may result in hacking, or make it a more attractive option. Through the categorization of specific indicators, our team was able to provide additional texture to our analysis by parsing out between necessary conditions (high categorizations) and supportive conditions (low categorization) as well as the difference between more direct indicators (direct categorization) and less direct indicators (indirect categorization) that produce cyber threat activity.

To begin our analysis, we rank-ordered the countries from 0-6 for each of the 60 determined indicators. A rank of 6 delineates that the country poses the biggest threat to cyber security in the specific indicator. A rank of 0 delineates that a country poses the lowest threat.[2]

This ranking system allowed us to assign a numeric rank to both the quantitative and qualitative data as seen in Tables 1.1 and 1.2.

Ranks are not forced. Therefore, if countries "tie" in a category they can both be ranked as the same number. Non-forced rank allowed us better ability to see the countries amongst one another and better determine their true cyber threat activity score. Additionally, it is important to note that the ranks assigned to each country are assigned comparatively among the six countries only and are not globally scaled. This means while one country may have received a 6 in a specific indicator when measured against the other five countries, this same country may receive a different rank for the same indicator when compared to other countries in the world.

The following chart is provided as an example for how we ranked the countries based on quantitative data. The table below shows the level of access to electricity in each country, one of the indicators that helped determine a country's *capability*.

Table 1.1

Country	**Access to Electricity %**	**Rank**
Indonesia	96	5
Malaysia	100	6
Philippines	87.5	4
Singapore	100	6
Thailand	100	6
Vietnam	99	5

Similarly, in table 1.2, we have ranked each country's "Cyber Enforcement" through the examination of arrests and laws on the books to determine which countries strictly enforce their cyber laws and thus, reduce threat.[3]

Table 1.2

[2] A rank of 0 was awarded in specific indicators when a country either showed no measurable presence in the indicator field or if research resulted in no information.

[3] We remain cognizant of the fact that these rankings, while grounded in research do involve judgments and are thus, subjective and non-agnostic.

Country	Cyber Enforcement	Rank
Indonesia	Moderate enforcement	3
Malaysia	High enforcement	1
Philippines	Low enforcement	5
Singapore	High enforcement	1
Thailand	High enforcement	1
Vietnam	Low enforcement	5

As previously mentioned, we categorized each indicator as either low, medium or high and direct or indirect. To perform a weighted calculation in our model, it was necessary to determine one total weight. The total weight was then determined for each of the indicators by determining all possible combinations of low, medium or high and direct or indirect. In our model, indicators received one of six weights:

1 = “low, indirect” 2 = “low, direct”
3 = “medium, indirect” 4 = “medium, direct”
5 = “high, indirect” 6 = “high, direct”

Total weights were assigned to indicators based on the indicators overall impact on cyber threat activity. “Low-high” measures the impact on cyber threat activity, while direct and indirect measures whether the indicator leads directly or indirectly to hacking. A "high, direct" indicator received the greatest weight (a weight of 6) as it has the largest direct impact on cyber threat activity. Conversely, "low, indirect" received a weight of 1 as it has the smallest and least direct impact on cyber threat activity. For example, “Screen Time” received a “low, indirect” weight as time spent in front of a computer, TV, or phone does not necessarily lead to or promote hacking. Further, “Culture” received a “high, indirect” weight as culture and the acceptance of hacking plays a high role in allowing for hacking, but does not directly cause it.

The indicators, in relations to their driver category and total weight can be seen in the graphic displayed on the following page.

To compare across countries, we then determined a minimum and maximum score. The minimum possible score is 0, which would result from a country earning minimal threat scores (0) in every indicator. The maximum possible score is 1,500, which would result from a country exhibiting perfect threat behavior (6) in every indicator.[4] We have presented our findings in ratio format. Therefore, the scores will be presented in a 0 – 1 ratio corresponding with the minimum and maximum threat scores of 0 – 1,500.

With this framework, we were then able to determine each country's cyber threat activity score by multiplying their unique indicator ranks by total weight and summing to determine their overall threat score.

Indicator Word Cloud

[4] Minimum score was determined by multiplying each total weight by 0 (least threatening) and summing the totals. This resulted in a minimum score of 0. The maximum score was determined by multiplying each total weight by 6 (most threatening). This resulted in a maximum of 1,500.

INDICATOR GUIDE

In this graphic, the indicators are categorized by total weight and sorted by driver.

HIGH, DIRECT = 6

Capability: Access to Electricity; Adult Literacy Rate; Cyber Competitions; Hour of Code; Internet Users; Strong Focus on Military; Trade Schools

Motivation: Domestic Politics; Geopolitics; Inequality in Income (SWIID Rank); Patriotism/Hacktivism; Spying; Unemployment Rate (Total and Youth)

Opportunity: Cyber Crime Arrests/Indictments and Enforcement; Informal Economy

Investments

HIGH, INDIRECT = 5

Capability: Culture; Cyber Militias; Formal Education (% of Enrollment); Hacker Conferences; Norms; Number of ABET Accredited Schools; Offensive/Defensive; Post-grad Employment; STEM Visa Enrollment %

Motivation: APT Groups; Previous Attacks; Pride/Ego; Website Defacements

MEDIUM, DIRECT = 4

Capability: CISCO and CompTIA Tech Certifications; Informal Education (Number of Videos); Malware in National Language(s)

Motivation: Curiosity; Religion

Gender: Gender Inequality Index

MEDIUM, INDIRECT = 3

Capability: CERT Conduct; Cyber Clusters; Cyber Policy; Fixed Broadband Subscriptions; GDP - per capita (PPP); Hacking Team Software; Internet Servers Using Encryption

Motivation: Blocked Access

Opportunity: Cyber Law

Gender: Population with at least some secondary education, male (% ages 25 and older, male and female)

LOW, DIRECT = 2

Capability: Bandwidth Production; Number of ISPs

LOW, INDIRECT = 1

Capability: Cyber Security Council; Declared Cyber Command; Freedom House Rating; IXP

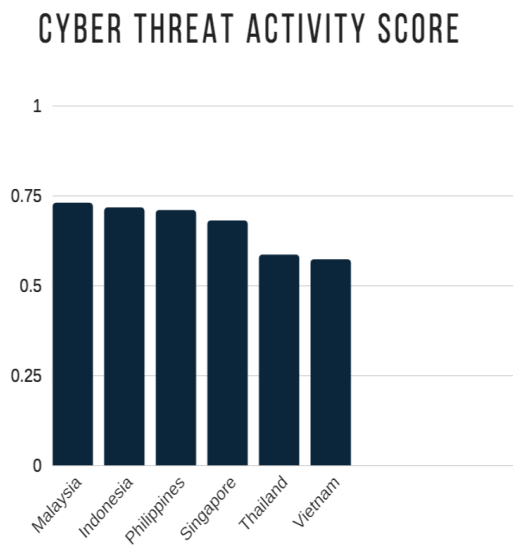
Motivation: Screen Time (Number of Hours/ Day/ Person)

Opportunity: Budapest Convention (Signed/ Ratified); Non-Align Movement (Member); UN Group of Experts (Member)

Gender: Gender Development Index

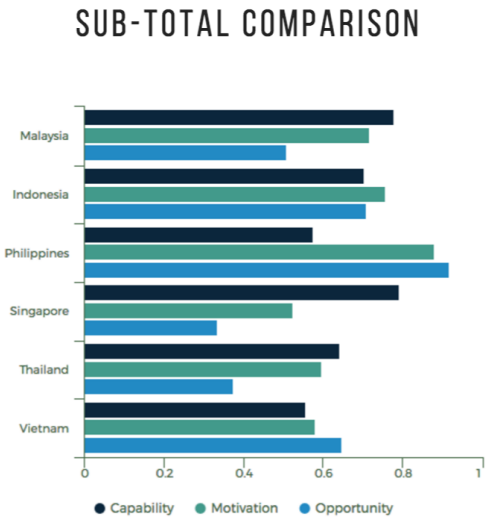
4. Results

After inputting the country ranks for each indicator into our model and multiplying them to determine a weighted cyber threat activity score, we recorded the following results:



These results indicate that the greatest threat in order of highest cyber threat activity to lowest is as follows: Malaysia, Indonesia, the Philippines, Singapore, Thailand and then Vietnam.

As previously discussed, the rankings were derived from a combination of *capability*, *motivation* and *opportunity* drivers. The agonistic nature of the *capabilities* driver led us to weigh *motivation* and *opportunity* drivers more heavily, as a country with *capability*, but without *motivation* and/or *opportunity* it is less likely to exhibit cyber threat activity. For example, while Singapore outscored all other countries in *capability*, the country was lapped in terms cyber threat activity due to low *motivation* and *opportunity* scores and ultimately placed 4th of the 6 countries examined. Conversely, the Philippines while scoring lower in *capability*, has high *motivation* and *opportunity*, which resulted in an overall 3rd place ranking. While the Philippines was not able to outscore Indonesia and Malaysia, as *capability* weighted less heavily, the country shows *high motivation* and thus gains a higher total cyber threat activity score. And lastly, Malaysia ranked among the highest across all three drivers and subsequently placed 1st as the country exhibiting the highest cyber threat activity. A visual depiction of this analysis can be seen in the graph below. [5]



In the country analyses that follow, we will detail the reasoning for these cyber threat activity scores by highlighting notable information gathered from our research.

5. Country Analysis

Our model produced a close but clear ranking of the six countries. Due to the varying range of scores, and the stratified results our data produced where a country was significantly higher in one driver but last in another, our team deemed it necessary to provide an analysis of each country to thread trends into a

[5] While the graphic in the sub-total comparison allows for a visual of the stacked drivers, it does not directly equate to the total cyber threat activity score, as the sub-total ratios cannot be directly compared to the total ratio.

narrative useful for our clients. This section will include graphics that detail the scores of each individual country in terms of our chosen drivers: *capability, motivation,* and *opportunity* in addition to a discussion outlining the notable *state* and *non-state* characteristics. Additionally, these country sections will provide insight on salient *drivers, barriers,* and

future considerations to provide a full view of each given country in terms of their relationship to cyber threat activity. The countries are presented in order of greatest cyber threat activity to the least.

Overview: Malaysia ranks 1st out of the six countries examined, indicating that Malaysia is the greatest cyber threat actor among these countries. Malaysia's 1st place rank results from the country's overall consistency of its scores within the *capability*, *motivation*, and *opportunity* drivers. Although Malaysia did not take 1st in all of the sub-total categories, the country's overall consistency between drivers allowed for the highest cyber threat activity score.

Malaysia's *capability* score was the second highest of the countries examined, falling just behind Singapore. Malaysia's high *capability* is expected, as Malaysia, in recent years, has revamped its education system by focusing heavily on developing research quality, expanding transnational education (TNE), and increasing the number of programs and courses related to technology and entrepreneurship.[6] This revamped effort to improve education has resulted in a higher *capability* score, as increases to education have allowed Malaysia's greater access to technology.

Malaysia's high *motivation* score stems from economic issues caused by the Asian Financial Crisis. Malaysia's recovery from the crisis has been slower than other Asian countries as a result of stimulus fund mismanagement and deep corruption.[7] As a result of these economic issues, income and wealth inequality in Malaysia is very high. High inequality has motivated Malaysian citizens to find other avenues, even those that are deemed illegal, including engaging in cyber threat activity.

Malaysia ranked 4th within the *opportunity* sub-total category. While Malaysians have sufficient *opportunity* to partake in cyber threat activity, the state does have strict cyber monitoring and control as seen in their policies, laws, and enforcement. Malaysia has proven capable of deterring cybercrime such as credit card fraud. For example, in 2016, 105 people were arrested in Malaysia as part of a credit card fraud ring.[8] While Malaysia is not perfect at enforcement, they do attempt to enforce laws and thus, the country's *opportunity* score is lower.

State: At the state level, Malaysia possesses strong institutional cyber conduct as seen by its scores in indicators such as: "CERT Conduct," "Cyber Policy," and "Cyber Security Council." Malaysia is the Permanent Secretariat to the Organization of Islamic Conferences – Computer Emergency Response Team (OIC-CERT).[9] Malaysia's role in the OIC-CERT may reduce threat activity, as state coordination against cyber activity has historically reduced threat activity. However, involvement in this specific CERT may indicate a willingness to partake in religiously motivated hacking. While this indicator is a "moderate, indirect" indicator, we wanted to highlight that this indicator may have an impact on the understanding of religious norms regarding hacking

[6] Betsy J. Bannier, "Global Trends in Transnational Education," International Journal of Information and Education Technology." 6:1, January 2016.
[7] Goh Soo Khoon, Michael Lim Mah-Hui, "The Impact of the Global Financial Crisis: The Case of Malaysia. *Third World Network.* 2010. http://www.thirdworldnetwork.net/finance/file_dir/12190611054dd0cf08a5bf8.pdf

[8] John Lyden, "Malaysia-based credit card fraud ring broken, 105 arrested," *The Register*. July 8 2016 https://www.theregister.co.uk/2016/07/08/credit_card_fraud_ring_busted/
[9] OIC-CERT, "Cybersecurity Malaysia Appointed As Secretariat to OIC-CERT," 2013. Web. https://www.oic-cert.org/en/newsletter.html

within the country. In regards to Malaysia's cyber policy and cyber security council, the government plays an active role in managing, improving, and defending its cyberspace. The government's active role reduces the *opportunity* for cyber threat activity within the country.

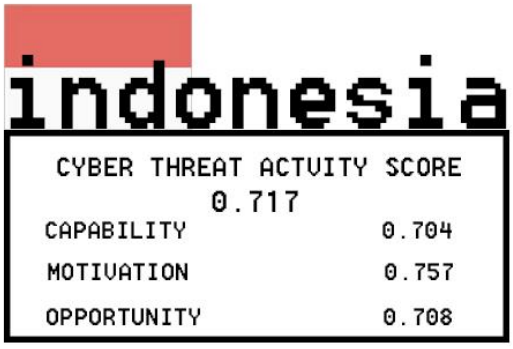
Non-State: Several religious-based hackers, such as Ardit Ferizi, who are affiliated with ISIS, have engaged in cyber threat activity within Malaysia.[10] Ferizi, and other non-state actors have been known to deploy malicious hacks ranging from online scams, and data theft and leakage, to more highly pervasive attacks. The growing presence of non-state actors may be a result of the growing number of informal education opportunities in Malaysia. Recently, there has been a growth in the number of hacker conferences, cyber clusters and trade schools in the country, signaling new paths for individuals to gain tech skills. These informal avenues influence the likelihood that citizens are able to obtain technological knowledge.

Additionally, non-state actors in Malaysia have been seemingly motivated by both geopolitics and patriotism/hacktivism. Malaysia has distinct geopolitical ties and tensions with China and other ASEAN nations that may likely be increasing cyber threat activity within the country as a way to address their national grievances.

Drivers: Malaysia's high cyber threat activity score results from a number of indicators. A mentioned above, at the non-state level, we found high participation rates in cyber clusters and hacker conferences. In addition, to these indicators, Malaysia's high cyber threat activity score also results from high numbers of participation in both formal and informal education paths such as tech universities and trade schools, which increase *capability*.

Barriers: While Malaysia came in 1st place, it did have a lower *opportunity* sub-total score than some of the other countries. As previously mentioned, Malaysia's numerous cyber laws and cyber arrests suggest the country has made securing its cyberspace a top priority. Additionally, the government's mandate to be globally recognized as a cyber-security powerhouse also highlights Malaysia's aspirations to enhance and guard its cyberspace. This growth in state-level security of cyberspace, serves as an *opportunity* barrier to cyber threat activity. Furthermore, Malaysia's informal economy and organized crime sector is among the lowest in the region with a negligible 10-15% of the population working in the informal sector, according to an OECD Malaysian Government report.[11]

Future Considerations: Malaysia's fast growing *capability* as result of increased formal and informal education and participation in hacker conferences and cyber clusters, coupled with growing motivation in the aftermath of the Asian Financial Crisis, may continue to cause more cyber threat activity from the country. However, as the government is taking steps to reduce opportunity and the black market is not as vast in Malaysia as in other nations, it remains to be seen whether or not activity will be diminished as a result of lower *opportunity* over time.



Overview: Indonesia ranked 2nd out of the six countries we examined. Indonesia placed 2nd in both *motivation* and *opportunity*, but placed 3rd in *capability*. Indonesia's scores in the following indicators, "Unemployment Rate – 5" and "Youth Unemployment Rate – 6" drove their *motivation* sub-

[10]Devlin Barrett, "U.S. Charges Man in Malaysia With Hacking Aiding Islamic State." The Wall Street Journal. Oct. 15 2015. https://www.wsj.com/articles/u-s-charges-man-in-malaysia-with-hacking-aiding-islamic-state-1444950858

[11] Department of Statistics Malaysia, Press Release: Informal Sector Work Force Survey Report, Malaysia 2015, (DoS Malaysia: 2016). Web.https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=UUFsUEJnNGFhcDE1TndNUlg4OEZCQT09

total score upwards. Indonesia has the highest unemployment rates among the six countries we examined. Weak education and little presence of cyber clusters reduced their *capability* score. With the largest economy in Southeast Asia, Indonesia has struggled to align its educational system to feed into the economy directly hence, Indonesia fell as a result to 2nd place, in overall cyber threat activity.

State: Indonesia's most significant state-level scores came from the following indicators: "CERT Conduct – 6," "Strong Focus on Military – 6," and "Declared Cyber Command - 6." As part of one of the only religious based CERT's, Indonesia's participation in the OIC-CERT is a testament to its interest in maintaining, and possibly strengthening its overall cyber capacities. While CERTs are seen as deterrents to cyber threat activity, Indonesia's involvement in a religious based CERT may shift the agenda of how they understand, and therefore respond to cyber threat activity. Additionally, Indonesia focuses heavily on their military, which extends to the cyber domain, as seen with the creation of the National Cyber Army. This entity signals the continuation of the country's value placed in the military, and the value placed in actively deterring cyber threat activity.

Non-State: Non-state actors in Indonesia have a host of opportunities given Indonesia's large black market and lax cyber enforcement and cyber laws.[12] As the chance of being caught for conducting malicious cyber activity diminishes, non-state actors may be incentivized to engage in such activity.

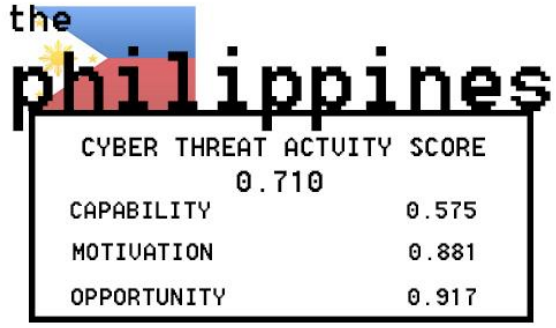
In Indonesia, we specifically observed religious cyber militias. This is intuitive for a country with high religiosity. Therefore, it was not surprising to observe several pervasive cyber militias organized around religion. These militias have even engaged with and worked alongside with other militant groups such as Hezbollah, a non-state, Islamist militant group.[13]

Drivers: Indonesia's overall score is predominately determined by its high *motivation* sub-total score, which was driven upward as a result of high activity in the indicators measuring patriotism/hacktivism and religion.[14] Furthermore, Indonesia's unemployment rates, specifically its youth unemployment rate, contributed to Indonesia's high *motivation* score.
Indonesia's large black market and informal economy serves as a breeding ground for its high *opportunity* sub-total score. This is caused by the unregulated and inefficient e-commerce sector. According the ILO, up to 60% of the Indonesian work force are in the informal economy.[15] While that percentage only indicates the number of people not registered in official statistics, it also highlights an overall willingness to participate in the informal economy. This willingness may be one avenue to engage in cyber threat activity, and may help explain the rise in cyber-crime in Indonesia in recent years.

Barriers: Although the Indonesian government has pushed to increase education spending and access to education, the country faces significant short-term and long-term challenges in educating citizens and providing jobs for graduating students. Indonesia has the highest percentage of youth unemployment of the six countries we examined. The country's inability to effectively promote STEM curriculum at the earlier grades significantly impairs the State's ability to increase overall cyber capacity.

Future Considerations: Indonesia's growing inequality in income and its inability to address its economic issues, such as youth employment, infrastructure weakness, labor shortage and skills mismatch between education and the job market may result in an uptick in cyber threat activity. Moreover, despite the government's initiatives to expand its critical infrastructure, the growth of the Internet within Indonesia outpaces Indonesia's aim to control it, inevitably giving birth to a space that the State may not be able to sustainably monitor or govern efficiently.

[12] Cyber Law Asia, "Cyber Laws in Asia," 2010. Web. http://cyberlawasia.com/cyber-laws-asia/
[13] Cyber Threat Insider Blog, "#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation," August 11, 2014. Web. https://blog.sensecy.com/tag/icr/
[14] Wibawanto Nugroho, "Indonesia and the globalization of religious terrorism," September 09, 2016. Web. http://www.thejakartapost.com/academia/2016/09/09/ri-and-the-globalization-of-religious-terrorism.html
[15] OECD, Structural Policy Country Notes Malaysa, (OECD: 2012), p. 4-7 Web. https://www.oecd.org/dev/asia-pacific/Malaysia.pdf



Overview: The Philippines ranked 3rd in our model, which, at first blush, seemed odd, as the Philippines' cyber activity does not suggest sophistication. The Philippines low *capability* score results from the fact that the country trails behind in training and retaining cyber security experts in comparison with the other five countries.[16] When we scratched beneath the surface, a host of indicators revealed the country to be moving in a direction that would alter this understanding dramatically. First, the country's lack of robust technological development, and its miniscule focus on STEM programs, actually makes the Philippines an attractive place to invest. Further, they have communicated intent to align to Western influences seen in the construction of similar organization of governmental structures tasked with cyber related issues. Additionally, the Philippines has been open about their intention to partner with other Southeast Asian countries to cooperate in cyber domains.[17] These characteristics push the Philippines in a direction where we've assessed their growing cyber threat activity. As discussed, we can begin to observe how *motivation* and *opportunity* indicators overshadow the Philippines' lack of *capacity*, communicating a desire to transform its image and technological future. Within our model, it was this *motivation* in tandem with a high *opportunity* score, as a result of poor enforcement, that boosted the Philippines to 3rd place.

State: The Department of Information and Communications Technology (DICT) works actively with the Cybercrime Investigation and Coordination Center. DICT is in charge of drafting cybersecurity plans, which delineate roles for traditional avenues of authority melding their mission under a cohesive framework.[18] What can be seen from this activity is the intent to connect, which is a critical component to responding when a cyber-breach is occurring or has just occurred. This can also help unify the state for growth in the future. As a result, the Philippines will likely be able to grow quickly, with cohesion, and without much debate – a critical component to strengthening cyber powers. The Philippines is also a member of the Asian Pacific Computer Emergency Response Team (APCERT), which only further highlights their desire to submerse themselves within a community of more sophisticated cyber actors where the transference of knowledge is quick.[19] Again, while they are not strong in terms of state power and do not have many matured formal institutions with proven capacity, they have proven themselves to be motivated, as they have laid out structures to manage cyber threat activity.

Non-state: The Philippines shows some malicious cyber activity within what seems to be non-state hacker group, even if these groups do not show high threat. In a recent case, "cyber cops" raided an Internet/online gaming café where a hacker group was reportedly "operating as a cybersex den."[20] The group was reportedly engaging foreigners who posed as women, but were male, in an online cybersex chat. While this is not necessarily illegal, law enforcement tracked the group and later found them to be blackmailing customers threatening to publish customer interactions if they were not given money. This example shows how the Internet is being utilized

[16] Jodesz Gavilan, "The state of cybersecurity in the Philippines," 2016. Web. http://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines
[17] Terakhir Dikemanskini. "Malaysia and Philippines established cooperation on cyber security," *Agenda Daily*. Dec 13 2016. Web. http://www.agendadaily.com/Business/malaysia-and-philippines-established-cooperation-on-cyber-security.html
[18] "Cybercrime Investigation and Coordinating Center (CICC) | DICT" Republic of the Philippines. Web. http://www.dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc/
[19] Graham Ingram, "Asia Pacific Computer Emergency Response Team APCERT," Web. https://pdfs.semanticscholar.org/96d1/b28092c394ce158fff058b8420852ed8f888.pdf
[20] Maan Macapagal, "WATCH: Men who pretend to be women nabbed in cybersex den raid" *ABS-CBN News*. July 28 2016. Web. http://news.abs-cbn.com/news/07/27/16/watch-men-who-pretend-to-be-women-nabbed-in-cybersex-den-raid

in ways for extortion purposes by groups engaging in illegal activity not necessarily cyber threat activity. Additionally, it showcases how enforcement is equally shifting to crack down on what erodes national and cultural values.

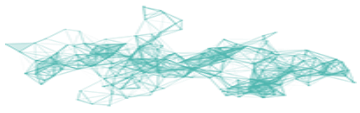
Drivers: The strength of the Philippines is undeniably their *motivation* and will to grow their cyber capabilities. This is not limited to cyber capacity, but overall economy as the Philippines has the fastest growing economy in the region to date.[21] While this does not stand in lieu of current *capability*, their attitude and proven momentum to develop relationships, allowing for investment for technologically based corporations to move into the area elevates the Philippines to the top three potential countries for cyber threat activity in our model. This level of *motivation* is so high it pushes the country to surpass Singapore, a much more capable and sophisticated country.

While domestic politics in country remain precarious, Philippines also possess a long history of geopolitical tensions with China, where we observe Chinese encroachment driving many of the state's grievances.[22] With this political atmosphere, coupled with the country's proven intent to increase cyber capacities, we anticipate an uptick in cyber threat activity.

Barriers: A notable example of their motivation to connect their population to technology is their educational program, Tech4ED. This initiative brings the Internet to rural areas to assist less socio-economically wealthy communities in developing computing skills necessary for an increasingly connected world.[23] This program is expected to increase what some experts have called "cyber hygiene," or the understanding of how to safeguard information online. Additionally, we can expect that an increase in technology education may assist in deterring and/or diminishing possible grievances from materializing within.

Additionally, the State has been active in producing policies to delineate specific tasks in the event of a cyber-security breach. This helps focus the state and provides the necessary conditions for building institutional memory. These kinds of actions traditionally serve as a barrier to cyber threat activity. Research revealed that the Philippines is not among the host of states to have bought software from Hacking Team; they, alongside Indonesia are the only two countries examined who have not yet purchased from this organization.[24] This suggests that the Philippines is not investing in surveillance and monitoring of citizens, which often leads to less cyber threat activity as this has proven to be a more positive characteristic of the state in the eyes of the populous. Finally, the Philippines does not have a strong focus on formally educating their population in STEM programs, meaning that the likelihood of citizens to develop skills necessary to cyber threat are lessened.[25]

Future Considerations: Future concern with the Philippines lies in the strategic balance of increasing connectivity without discouraging the development of expertise while also eliminating the necessary conditions that produce malicious cyber activity. How the Philippines develops their cyber capacity and how their grievances with China and other geopolitical grievances manifest should also be closely monitored. It will be interesting to see if an increase in technological innovation will influence military capacity, and whether this will embolden the Philippines and Filipino non-state actors to take stronger, further, and more devastating actions against those they perceive to be a threat.



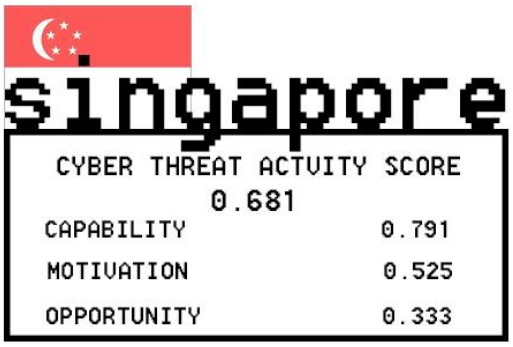
[21] Yap, Karl Lester M, "Rising Tiger Philippines Posts some of the World's Fastest Growth," Bloomberg. https://www.bloomberg.com/news/articles/2017-01-26/asia-s-new-growth-leader-takes-over-from-fading-tiger-economies

[22] Simone Orendain, "Philippines Files Pleadings in Case Against China," *VOA* March 30 2014. Web. http://www.voanews.com/a/philippines-files-pleadings-in-case-against-china/1882322.html

[23] "Tech4ED Platform | eSociety - Information and Communications Technology Office." Republic of the Philippines. http://dict.gov.ph/tech4ed/tech4ed/tech4ed-platform/

[24] "Mapping Hacking Team's "Untraceable" Spyware." Citizen Lab. February 17 2014. Web. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[25] Neil G. Ruiz, "The Geography of Foreign Students in U.S. Higher Education: Origins and Destinations." *Brookings Institute.* August 29 2014. Web. https://www.brookings.edu/interactives/the-geography-of-foreign-students-in-u-s-higher-education-origins-and-destinations/



Overview: Singapore ranked 4th out of the countries we examined. While Singapore ranked 1st in *capability*, its low scores in *motivation* and *opportunity* place Singapore behind the other countries. High *capability* is unsurprising as Singapore has among the strongest scores in formal education, encrypted servers and general capacity indicators. In essence, Singapore's *capability* is most directly driven by the state's cyber policies, cyber council score and cyber clusters. However, Singapore lacks in *opportunity* and *motivation*, notably because cyber enforcement and cyber laws act as effective deterrents to malicious cyber activity.

State: Singapore has the highest GDP per capita score as well as the highest overall score in *capability* among the surveyed countries.[26] The state has also encouraged investment into cyber security and continues to develop strategic cyber policies, recognizing the growing importance of the field. In this regard, the low scores for "Cyber Enforcement – 2," and "Cyber laws – 2," indicating lack of threat, are not surprising, as Singapore has maintained a tightened grip on cybercrime activity, as this activity may threaten the economy—intuitive for a country largely dependent on financial services. We surmised that Singapore's low *motivation* may be attributed to an overall sense of stability, which comes with the privilege of a stronger economy, and less tense relationships with its neighbors.[27] In short, Singapore is less motivated to engage in cyber threat activity as a result of stable geopolitics, as its neighbors pose less of a threat to their overall sovereignty.

Non-State: Non-state actors in Singapore face several challenges to conduct malicious cyber threat activity. Cyber laws and their strict enforcement act as an overall deterrent and, in Singapore, strict enforcement by authorities has continued to grow in recent years. Additionally, general restrictions outside the formal economy and the lack of a clear organized black market makes it hard for actors from inside the city-state to engage in cyber threat activity on a major scale. The lack of *opportunity* and *motivation* is significant, as exemplified by the low scores Singapore received in both *key motivation* and *opportunity* drivers.

Drivers: Singapore ranks 1st in *capability* due to a number of indicators, in which it performs strongly, such as: Investment, Clear cyber policy and high scores in formal education. These *capability* indicators are important drivers to emanate cyber threat activity as they speak to the country's overall understanding and insight into cyber space.

Another set of strong drivers results from the country's low "Freedom House Ranking – 3," and contested "Domestic Politic Ranking – 3," which has resulted in some citizens using illicit means to voice their opinions. These Drivers also spur heightened hacktivist activity, which has become more sustained in recent years.

Barriers: Singapore scored lower in "Curiosity – 4" and "Norms – 2," as experimental hacking is highly discouraged by both the government and general public opinion. In essence, curiosity is only encouraged in government spaces, within university programs, and occasionally encouraged in cyber competitions. These scores function as an important deterrence to the detection of offensive talent. Taken together with the scores in cyber enforcement and laws, these act as important barriers that lower cyber threat activity, as they significantly decrease overall scores in *opportunity* and *motivation*.

Future Considerations: Singapore continues to invest heavily in cyber security and capacity recognizing the

[26] "Singapore," *Forbes.* 2017. Web. *https://www.forbes.com/places/singapore/*
[27] Gabriele Giovanini & Emanuele Schibotto, "Singapore and the Asian Century", February 19 2015, http://thediplomat.com/2015/02/singapore-and-the-asian-century/

dependence of the economy on new technology.[28] However, if contested domestic policies and restrictions on the freedom of expression persist, there might be a future rise of hacktivist activity.

Overview: Thailand ranked 5th out of the six countries we examined. Thailand placed 4th in both capability and *motivation*, but fell behind in *opportunity*, where it placed 5th. An overall lack of *opportunity* is unsurprising as Thailand has some of the strictest laws in the world regarding malicious cyber threat activity. In addition to moderate *capability* and *motivation* subtotals, the significant lack of *opportunity* in Thailand was the biggest barrier that diminished its cyber threat activity score.

State: Thailand's highest state scores came from "Offensive/Defensive - 6" and "Strong Focus on Military - 6." The newly approved cyber security strategy of 2016 explicitly speaks about building up cyber weapons and capabilities that can be used offensively and even increase deterrence for future combats. Additionally, Thailand is the only country of the six countries we examined that has an explicitly stated offensive cyber strategy. Overall, the state, by way of the military has been a driving force of cyber development after recent attacks aimed at government services and websites.

Non-State: Non-state actors in Thailand have very little *opportunity* as the laws are very strict and create a high *opportunity* cost for hacking. Major cases like that of Pongsak Sriboonpeng, who was condemned to 60 years in prison, under Article 112 of the Code of Conduct, for defaming the King on the Internet, serve as a deterrent to cyber threat activity.[29] While the Article 112 laws indirectly apply to cyber threat activity, as they specifically concern defamation of the King, they are an extension of Article 14 of the Computer Crimes Act.[30] This tertiary use of law to affect cyber actions has created a state in which cyber activity is highly scrutinized. This level of scrutiny has resulted in many arrests for hacking under the 2007 Computer Crimes Act and even the arrest of international citizens for cyber fraud and theft, highlighted by the arrest of Russian citizen, Dmitry Ukrainsev.[31] Additionally, Thailand has a great deal of social surveillance that deters activity. Groups like the Rubbish Collection Organization and Cyber Scouts, a youth group, monitor Thai citizens and turn in those who defame the King online.[32] The combination of strict and vastly applied laws and social surveillance may diminish the attractiveness for non-state actors to cyber threat activity.

Drivers: Thailand's score comes from a variety of capacity and *motivation* indicators. For example, CompTIA Certifications are available in Thai. CompTIA is not available in any of the other five country's national languages - excluding Chinese and English.[33] Additionally, the CompTIA exams are even serving as the final exams for students at the Thai-Nichi Institute of Technology, a private institution founded in concert with Japan with extensive information technologies tracks.[34] The proliferation of

[28] Liz Gannes, "Singapore Rising: The Plot to Be The Next Big Tech Hub", Jun 16, 2015. Web. https://www.recode.net/2015/6/16/11563586/singapore-rising-the-plot-to-be-the-next-big-tech-hub
[29] "Running Afoul of the Thai Monarchy." The New York Times. September 17, 2015. Accessed April 19, 2017. http://www.nytimes.com/interactive/2015/09/18/world/asia/thailand-king-lese-majeste.html.
[30] Nathan, David. "Thailand's youth asked to cyber-spy for the state." New Internationalist. Accessed April 19, 2017. https://newint.org/features/web-exclusive/2014/09/05/thailand-cyber-crackdown/.
[31] "Thai police arrest Russian, Uzbeki for alleged cybertheft." Phys.org - News and Articles on Science and Technology. July 21, 2016. Accessed April 19, 2017. https://phys.org/news/2016-07-thai-police-russian-uzbeki-alleged.html
[32] Nathan, David. "Thailand's youth asked to cyber-spy for the state." New Internationalist. Accessed April 19, 2017. https://newint.org/features/web-exclusive/2014/09/05/thailand-cyber-crackdown/.
[33] "CompTIA Thailand." CompTIA Information Technology. October 2012. Accessed April 19, 2017. https://www.comptia.org/international/thailand/home.
[34] Thai IT Students Gain Competitive Edge with CompTIA Certifications. December 1, 2016. Accessed April 19, 2017. https://certification.comptia.org/it-career-news/post/view/2016/12/01/thai-it-students-gain-competitive-edge.

these exams creates a better-trained population more capable of producing cyber threat activity.

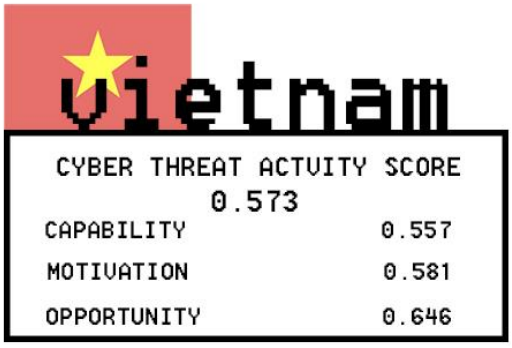
Thailand is also one of the only countries we observed to have encountered malware in its national language. We have recorded several example of malware in Thai. In this case specific Thai phrases and language patterns were detected that are tailored to specific programs and machines used in Thailand.[35] This malware drives Thailand's cyber threat activity score upward as it shows an advanced understanding of computer language adaptation.

Barriers: Formal Education in Thailand is not as robust as the other five countries. The "Percentage Enrollment - 3" in Thailand brought down the overall capacity score as Thailand has many online universities with open enrollment. While their percentage of enrollment is high, the number at face value is misleading due to the nature of the enrollments.[36] Additionally, Thailand has one of the lower percentages of STEM Visa students studying in the U.S. Thailand ranks 38th out of 74 and 5th out 6 within the six examined countries.[37] This lack of formal education indicates a capability gap that may exist within the country.

Additionally, Thailand has low levels of unemployment and income inequality. Of the countries examined, Thailand has the lowest income inequality. Low unemployment and inequality is a positive aspect for the country overall, which drives down Thailand's cyber threat activity score as low unemployment and high income equality reduce *motivation*. A sense of equality in both social class and gender fosters a community of satisfied citizens, reducing discontent, and thus diminishes motivation to hack.

Another barrier for Thailand are its scores in the following indicators: "Cybersecurity Council - 0" and "Declared Cyber Command - 0" as it has developed neither of these cyber units. While Thailand has an intricate hierarchy of digital governance, the proliferation of cyber architecture should not, however, indicate cyber sophistication. As Kan Yuenyong, Director of Siam Intelligence Unit Think-Tank stated, "[t]he military's definition of 'cyber attacks' is too broad… and 'the military may not thoroughly understand cyber security."[38] Additionally he stated, "[c]yber technology may not be advanced enough to handle missions as expected."[39]

Future Considerations: Thailand is planning substantial growth in both development of state policies and citizen capacity. They are also investing in building their cyber strength and may eventually earn a higher score. It will be necessary to consider how traditional laws influence the direction that Thailand takes in terms of this future investment.



Overview: Vietnam trails behind all five of the countries in our examination of cyber threat activity. Vietnam scored the lowest in *capability*, and *motivation*, however, surpassed both Thailand and Singapore in *opportunity*. A higher *opportunity* sub-total score is largely due to the lack of state cyber coordination and direction. While other states may possess weak or over-exaggerated cyber infrastructure, research reveals that Vietnam ranks

[35] "Thailand faces big risk from malware." The Nation. October 28, 2015. Accessed April 19, 2017. http://www.nationmultimedia.com/news/national/aec/30271838.; "RIPPER ATM Malware Linked to Thailand Heist." Information Security News, IT Security News & Expert Insights: SecurityWeek.Com. Accessed April 19, 2017. http://www.securityweek.com/ripper-atm-malware-linked-thailand-heist.

[36] "Education in Thailand," World Education Services. March 3 2014. Web. http://wenr.wes.org/2014/03/education-in-thailand

[37] Ruiz, Neil G. "The Geography of Foreign Students in U.S. Higher Education: Origins and Destinations | Brookings Institution." Brookings. July 29, 2016. https://www.brookings.edu/interactives/the-geography-of-foreign-students-in-u-s-higher-education-origins-and-destinations/.

[38] "Many wonder about the extent of cyber army's jurisdiction." The Nation. October 26, 2015. http://www.nationmultimedia.com/news/national/aec/30271668.

[39] "Many wonder about the extent of cyber army's jurisdiction." The Nation. October 26, 2015. http://www.nationmultimedia.com/news/national/aec/30271668.

among the last in cyber maturity of countries examined.[40] Their lack of *capability* has proven to be a significant barrier to cyber threat activity in country despite having substantial *opportunity* to engage in cyber threat activity.

State: As the data indicates, Vietnam shows low intention to build state capacity and lacks organization wherein authorities are clearly defined and divisions are organized to coordinate on cyber related issues. Without a clear cyber policy, a cyber-council, or cyber command, the role of the state is limited to enforcement, which stems from their traditional enforcing bodies.[41] Vietnam is a consumer of software from Hacking Team, which indicates their desire to possess surveillance and monitoring capabilities. It is thought this may allow for better enforcement of law and thus, lower *opportunity*. Overall, their attainment of this software indicates a desire to have the opportunity to enforce, but perhaps through a non-traditional path, as they have not created other strong avenues for deterrence.

Non-state: According to FireEye iSIGHT reports, APT OceanLotus may be an operation of Vietnamese non-state actors, or potentially even state actors.[42] Using standard attribution techniques and indicators that delineate the timing of attack incidents, FireEye iSIGHT warns that there are likely Vietnamese roots within the group APT OceanLotus. As reported by leading cyber threat experts in the field, China has also reportedly been hit by OceanLotus with a three-year espionage campaign. This evidence contributes to the confidence that Vietnam may be connected intimately with this group.

Drivers: VN-CERT is increasing their capacity, growing to about 500 technicians on hand.[43] Despite this new development, it is unclear how effective Vietnam's CERT will be in the near future. As of now, we were forced to draw conclusions that while VN-CERT is active, it is still in its nascent stages and may not assist in consistent, and consorted active deterrence, as of now, although CERT presence may typically serve as deterrence. This, we argue contributes to the attractiveness to engage in cyber threat activity.

Additionally, Vietnam has some of the highest levels of screen times between the six examined countries. Like other countries, Vietnam is also investing in the integration of technology into services and structures. These indicators suggest that the State and its citizens are becoming more connected, and looking to increase integration of systems online. Without governmental coordinated structures; however, cyber threat activity may also increase in attractiveness, as groups or individuals may see opportunity in Vietnam to carry out disruptive activity with high success and low risk.

While Vietnam came in 6th place, there are particular aspects within the country that drove up their cyber threat activity score. For example, Vietnam scores very high in "Informal Education," as they have a number of technical trade schools that are teaching citizens coding techniques. Most notably, Coder School, a school started by Vietnamese citizen who attended Berkley and Yale seeks to train citizens and proliferate technical knowledge.[44]

Additionally, formal education in Vietnam may serve as a long-term driver to cyber threat activity. Vietnam is working with U.S. universities, such as Arizona State University, to expand technical knowledge throughout the country.[45] Additionally, the country has integrated technological and computer education into elementary, or primary schools.[46] While these initiatives, are good for the country, the more people that learn coding; the more capability that exists to carry out threats.

Barriers: While Vietnam may trail behind many of its neighbors in terms of possessing a strong system to

[40] Cyber Maturity in the Asia-Pacific Region 2016. Australian Strategic Policy Institute. International Cyber Policy Centre. 2016. Web. https://www.aspi.org.au/publications/cyber-maturity-2016/ASPI-Cyber-Maturity-2016.pdf
[41] "Country: Vietnam." The Software Alliance. Asia-Pacific Cybersecurity Dashboard. 2015. Web. http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_vietnam.pdf
[42] Chinese Firm Outs "OceanLotus Group: A Nexus with Vietnam? FireEye iSIGHT Intelligence. April 29 2016. Print.
[43] "International drill on cyber security held in Vietnam," VietNamNet. March 3 2017. Web. http://english.vietnamnet.vn/fms/science-it/175099/international-drill-on-cyber-security-held-in-vietnam.html
[44] "About CoderSchool." CoderSchool. http://www.coderschool.vn/about
[45] Obama highlights ASU during trip to Vietnam. ASU Now. May 26 2016. Web. https://asunow.asu.edu/20160523-global-engagement-obama-mentions-asu-during-trip-vietnam
[46] Secondary education in Vietnam*

address cyber threats and re-establish secure systems in the case of a breach, the country has clearly outlined channels of cyber enforcement, which serve as deterrent to cyber threat activity. The Ministry of Information and Communications coordinates and seeks to prevent and deter from cybersecurity violations; the Ministry of National Defense focuses on violations against national sovereignty; and the Ministry of Public Security focuses on cybercrime and interacts with Interpol.[47] Despite having passed the first cyber related policy in 2016, Vietnam's enforcement is outlined and coordinated. This is expected, as Vietnam has possessed a strong focus on military prior to the integration of cyber tools.

Future Considerations: More research must be done on Vietnam in order to discern whether the country will take a more government controlled approach or allow for gradual development of cyber activity. Vietnam ranked moderately high in "Informal Education" overall, with high numbers of YouTube videos that focus on teaching components of cyber activity.[48] Along with technical trade schools, and a moderately high number of "Hour of Code" events, Vietnam can be expected to increase exponentially in technical capacity should the country retain its citizenry. If so, the government and the people will need to carefully determine how they wish to establish the balance between security and privacy.

Considerable attention to how investment impacts Vietnam's economy and what entities are in control over information is paramount. According to the OECD, Vietnam has considerable amounts of investment in energy, which will require network systems to operate. Only time will tell if their new policy is capable of handling the inpouring of economic attention Vietnam is expected to receive in the near future.

6. A Closer Look

In this section, we chose a select number of indicators that stood out in our research. The indicators chosen, we believe, require closer examination as they have revealed to shift our analyses and raise further inquiries within our team's discussions. These boxes are not intended to predict cyber threat activity, but rather, flesh out the logic and direction of a particular indicator. That is, the breakout boxes are snapshots of considerations of how a particular indicator may shift our attention regarding activity.

Patriotism/Hacktivism

In our analysis, we used the indicator "Patriotism/Hacktivism" in one combined score in order to help rank the motivation of actors. After interviewing several experts on the matter, we were certain that singular analysis of these factors would only capture a part of the motivation. Thus, we included both indicators into one single framework, allowing us to capture a broader range of phenomena without having to make a final judgment call.

A good example of "Patriotism/Hacktivism" activity is provided by the 2014 cyber exchange between two groups from Malaysia and Indonesia. These groups defaced websites and hacked each other's university infrastructure by switching lights on and off.[49] What started as an innocuous competition quickly grew to possess patriotic flares, leading to the involvement of Anonymous.[50] This led Malaysia to pass new cyber legislation to encompass hacking cases like this.[51]

Religion

Religion plays a significant and unique role in a few of the countries our team has examined for both state and non-state actors. Religion was considered

[47] Lexology, "Data Security and Cybercrime in Vietnam," Global, Vietnam. 8, February 2017. Web. http://www.lexology.com/library/detail.aspx?g=37d6b3a7-f0aa-4a3f-8688-2e31967b1708

[48] "K-Team" YouTube Channel. 2017. https://www.youtube.com/channel/UCBw4b26KZrBvHRPBjOCw6UQ/videos

[49] Indonesian hackers launch Independence Day attack on Malaysian Websites, networksasia, http://www.networksasia.net/article/indonesian-hackers-launch-independence-day-attack-malaysian-websites-1251878483

[50] Niluksi Koswanage, "Malaysia tries to stop threatened Cyber Attack", Jun 15 2011, http://www.reuters.com/article/us-cyber-malaysia-idUSTRE75E05N20110615

[51] Ibid.

first in terms of how it is internalized by a population, then how it is practiced, as well as how its presence is woven into the politics. Additionally, we examined religious based grievances.

Multiple examples were found where religion likely contributed to cyber threat activity. Hacking can be motivated by religious factors and can be seen as a vehicle or tool for religious advocacy and practice. While we cannot determine whether a particular religion drives cber threat activity more or less, we do note several instances where attacks against a variety of targets were explicitly based on religious beliefs.

Religiosity is complex. It is unclear what is possible to know without immersing ourselves into the culture. That is, we were unclear whether our limited foresight was due to a lack of engaging sufficiently in Indonesian religious culture or resulted from other factors. For the purpose of clarity, we carefully attributed weights, discussed limitations, inquired often with experts and scanned for proxy examples to learn how religion was invoked in a country and at what times. While there is not a clear motivating direction religion plays in any one of these countries, we maintain that religion does play a role in cyber threat activity.

Education

In our analysis, we used Formal Education as an indicator to rank the capability of both non-state and state actors. Education was a top metric for measuring capability. We used the percentage of higher education enrollment and matriculation for each country to gather a quantitative outlook of each country's capability. Our simple assumption is that higher enrollment leads to higher potential capability. While percentage of enrollment was informative it was also limited in telling the whole story.

Our ranking based on percentage of enrollment does not include quality of education, number of STEM programs and course offerings, the changing educational investment climate, GDP expenditure towards each country's educational system, and foundational tangible skills acquired during the earlier years of schooling.

We included these details in post-graduate employability. Lower scores were generally given to countries which had a poor educational system, lack of resources, and outdated curriculum. Combined, our quantitative and qualitative metrics of education provided us with a holistic perspective which enabled us to determine the capability of each country.

Investment

Investment in Southeast Asia as a region has been an ongoing project. States and institutions with more economic power have been looking to develop markets, assisting in the development of certain markets within Southeast Asia. Similarly, countries within the region have been seeking to develop more dynamic and stronger economies to become more prosperous.

As the world becomes more interconnected and moves more online, investment in cyber technologies is not reserved exclusively for the state, or non-state actors, but always implicates businesses, which operate in-country. Therefore, as some of these countries open themselves up to investors, they must be able to secure and ensure that operating in country does not pose a significant threat.

Predicting how investment influences cyber threat activity deserves a closer look. Further, what type of investment that is itself undergoing technological innovation may be doubly vulnerable, even if it means cutting costs on producing in country. Investment, as an indicator, proves to be multifaceted in our work, and certainly important to include within our model. However, without understanding its ontological relationship with other indicators precisely, all we can conclude is its significance, especially in predicting future cyber threat activity.

Geopolitics

Early in our research, geopolitics proved to influence a country's general motivation for cyber threat activity. Leading scholars and researchers agree that major cyber-attacks and espionage are conducted in a tense international environment drawing more scrutiny to the underlying dynamics of state conduct.

Even citizen groups and individuals may become motivated by the geopolitical environment and lash out at foreign targets when they feel their country's reputation has been tarnished. This observation gives rise to consider nationalism as a potentially rich area of inquiry when looking at cyber threat activity. In this way, we can observe how patriotism and hacktivism are connected to a country's geopolitical situation.

A telling illustration of this factor has been demonstrated by several groups in the Philippines which lashed out at Chinese websites and attacked the availability of servers and forums for Chinese Internet users, after clashes over sovereignty in the South China Sea.[52]

In our analysis we found that tense geopolitical environments are accompanied by more cyber threat activity making it as an important indicator that should be closely watched in the overall *motivation* drivers.

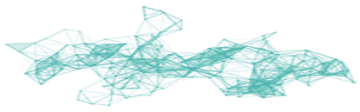
Rule of Law

In our analysis, we not only examined written law, but also law enforcement, as it is often the case that written law goes unenforced. Examining cyber arrests produced interesting results and informed our analysis for future hypothetical scenarios. If rule of law in the region changes, we can expect that cyber threat activity will likely fundamentally look different as a result. The analysis that rule of law alters activity emerged from examination of the stark contrast between the Philippines and Thailand.

In the Philippines, as previously mentioned, laws are very relaxed. The Philippines is even notorious for hacking due to great access to the black market as a result of lax money laundering laws.[53] If the Philippines were to conform based on international pressure and not only write, but also enforce laws that diminished opportunity, Philippines may pose less of a cyber-threat risk in the future.

Conversely, Thailand has very strict laws regarding defamation of the King and cyber activity. Article 112 of the Criminal Code, the Lèse-majesté laws, prohibit defamation of the King.[54] While these laws do not directly target hacking, they have created a culture of high social surveillance and thus, diminished opportunity. Additionally, Thailand has prosecuted many individuals under the 2007 Computer Crimes Act, as seen by the arrest of 40 individuals under this act in 2016.[55]

If other countries, begin to employ strict laws whether directly or indirectly related to cyber activity, we may see less cyber threat activity from the region.



7. Challenges

[52] (UPDATE) Filipino hackers fight back, deface Chinese sites, INQUIRER.net, http://technology.inquirer.net/10235/filipino-hackers-fight-back-deface-chinese-sites

[53] Chalmers, John, and Karen Lema. "For bank heist hackers, the Philippines was a handy black hole." Reuters. March 21, 2016. Accessed April 19, 2017. http://www.reuters.com/article/us-usa-fed-bangladesh-philippines-idUSKCN0WM13B.

[54] "Privacy International." Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand. September 20, 2016. https://www.privacyinternational.org/node/935.

[55] "UNCT, Thailand Submission." Universal Periodic Review. May 25, 2016. https://www.upr-info.org/sites/default/files/document/thailand/session_25_-_may_2016/rco_upr25_tha_e_main.pdf.

While our research has revealed a wealth of information there are particular challenges that influenced the analysis and should be addressed in future research into the area.

A. Language

Language was a challenging data point to integrate into our analysis given each country's demographics. For example, Singapore has four official languages: Bahasa Melayu, English, Mandarin, and Tamil. We looked at malware in national language and informal education taught in native languages but our insight was limited because we were unable translate and interpret several resources. In addition, while several of the country's' official language was not English, English was taught heavily in school or the language of instruction for higher education.

There weren't statistics on the number of English speakers in each country. However, language was a critical factor to determining each country's *capability*. Threat analysis must consider language as often cyber communities and cyber-crime groups have traditionally been established around language. Our research and expert interviews have suggested that language is a key cue to measuring *capability*.

B. Weighing

While we adhered to high academic standards and insights provided by experts, we assert that all weighing is inherently subjective. We sought to balance this with providing country analysis and delving heavily into qualitative research.

When it came to our model, subjective judgments were made based on qualitative data (such as norms, hacking culture etc.) while quantitative data was taken at face value. However, through the peer review process, within the team, and reviews and guidance from our faculty advisor, we believe we achieved the highest level of neutrality possible.

C. YouTube Analysis

Coding and Computer Science self-learning tutorials on YouTube or other online streaming providers only provide basic statistics on the watched video sites.

In order to understand where the people who watch YouTube video are located, you must be the owner of the video. This limits the ability for thorough research and downgrades the information that can be drawn. As we were unable to find this information, we tallied the number of YouTube videos available in each country's national language. However, as mentioned in Challenge 1, this again was difficult. Overall, using YouTube Analysis in combination with other indicators allowed us to draw a more comprehensive picture.

D. Proprietary Information

As we conducted our research, some of the information we attempted to gather was deemed proprietary information. For example, at first, our goal was track the number of CompTIA certified individuals within each country. However, after reaching out to CompTIA, we learned this information was proprietary. Instead, we focused on whether CompTIA exams were available in a country's national language. While this final indicator holds less specific information, it still provides an indication of the availability of exams within the countries.

During the research process, we pivoted around proprietary information and found new ways of capturing needed information. However, as there is untapped information in these areas, we recommend further research be conducted to gain a more holistic view of these proprietary indicators.

E. Gender/Investment

Gender and Investment were two indicators we ascribed as independent drivers that form their own drivers' component, as they were difficult to place under *opportunity*, *capability* or *motivation*. In essence our Gender score symbolizes several factors at once, participation rate for women in the economy (which could lead some women to turn to illicit means of making money), education of women (speaking to

their overall capabilities) and the cultural restraints or restrictions imposed on women. While it is an interesting vector, further research is necessary to draw a more complete picture. We chose to limit this research, as further examination requires more time and attention that was not available given our aims.

The "Investment" indicator suffers from a similar issue as "Gender", as it is hard to differentiate between state-driven, state-led and private investment. As we only had access to overall numbers of investment into information technology, cyber security and specifically for cyber clusters, it was difficult to determine accurate metrics and sources of investment.

In essence we treat investment as a driver that enables more cyber threat activity, as well as a useful prediction for the future of a country. Additionally, we also considered foreign investment and observed the areas it was intended to impact i.e. critical infrastructure, education, or otherwise. Thus, we use investment into the sector as an overall driver as a way for state and non-state actors to gain more access to technology and new systems as well as better education.

8. Conclusion

In terms of cyber threat activity Southeast Asia, as a region, is on the move. The six countries surveilled, each with unique values, ideas, and tendencies, showcase their distinct cyber development observed today. While our research has revealed crucial differences between the six countries and even within countries, as captured by our model, interesting trends have emerged. Analysis of the overall trends within the Southeast Asian region reveal certain driving factors that trigger cyber threat activity may make the difference between threat and non-threat. This, we believe is due to our flexible model fashioned to be applied to any region in the world – an important tool in an increasingly connected world in need of security.

Throughout the region examined, we observed the desire to grow investment, proliferate cyber policies, and increase connectivity. Increased connectivity and capacity has allowed for broader use of the cyber domain. These desires, compounded with outside influences and growing usage, have revealed the ways in which both governments and citizens have approached the cyber domain and utilized it for their own purposes – sometimes maliciously. With ranging, but overall high rates of investment in the region, we can confirm Southeast Asia will remain relevant in the years to come.

As we observed the cyber domain's use changing, dependent on the user and situation, a key take away is that *motivation and opportunity* should be prioritized over *capability*, despite the amalgamation of these key drivers that together make the necessary conditions for the production of cyber threat activity. While the *capability* driver outlined necessary infrastructure needed to hack, *motivation* and *opportunity*, as completely qualitative indicators, provide a more in depth analysis of the situation and help determine why and under what conditions malicious activity may occur. An examination of *motivation* on its own, elevated our analysis, allowing us the ability say more about what, where and when malicious actors are likely to strike. These indicators pushed our understanding of the underlying factors that drive actors to engage in malicious activity.

Examining *opportunity* allowed for a more interesting examination of the region, as it highlights on the ground maneuvers intended to diminish cyber threat activity. As discussed in previous sections of the report, all countries examined have implemented harsh or at least punishing cyber laws that aim to deter cyber threat activity. Knowing how they diminish or onset grievances is imperative to the drivers within this category.

Overall, this report provides a method to indicating cyber threat activity and charts the production of such a model. Our contribution to cyber discourse is one that prioritizes informed and fact-based examinations of Southeast Asia – a region is placing itself firmly on the cyber threat map.

9. Ranking Rationale

As we recognize that our rankings result from subjective judgment, we have provided the underlying research rationale that informed our rankings below.

CAPABILITY INDICATORS:

Access to Electricity – Malaysia, Singapore and Thailand received a score of 6 as they have 100% electrification. Vietnam and Indonesia received a score of 5 as they have close to 100% electrification (99 and 96 respectively). The Philippines received a score of 4 as it has 87.5 percent electrification.

Bandwidth Production – The countries were ranked in descending order dependent on their level of bandwidth. The country with the most bandwidth, Singapore, received a 6. The country with the least bandwidth, Malaysia, received a one.

Fixed Broadband Subscriptions – The countries were ranked in descending order dependent on their number of fixed broadband subscriptions. The country with the most subscriptions, Singapore, received a 6. The country with the least subscriptions, the Philippines received a 1.

Internet Servers Using Encryption – The countries were ranked in descending order dependent on their number of servers using encryption. The country with the most encrypted servers, Singapore, received a 6. The country with the least encrypted servers, Vietnam, received a 1.

Internet Users – The countries were ranked in descending order dependent on their number of Internet Users. The country with the most Internet users, Singapore, received a 6. The country with the least Internet users, Indonesia, received a 1.

IXP – The countries were ranked in descending order dependent on their number of IXPs. The country with the most IXPs, Indonesia, received a 6. The countries with the least number of IXPs, Malaysia and the Philippines, received a 1.

Numbers of ISPs – The countries were ranked in descending order dependent on their number of ISPs. The country with the most ISPs, Indonesia, received a 6. The country with the least ISPs, the Philippines, received a 1.

Adult Literacy Rate – All countries received a 5 in Adult Literacy Rate. Countries scoring between 90-99 received a 5. As all countries were in this margin, they received the same score.

Cyber Clusters – This indicator was a qualitative indicator. Therefore, we have provided specific justification for each country's ranking, in order of highest cyber threat activity score to lowest cyber threat activity score, below.

Malaysia received a rank of 6 because the cyber cluster "CYBERJAYA"[56] is specifically aimed at cyber capabilities both defensive and offensive, as well as the intention to build several more in the next couple of years. This cluster is the most active of all clusters in the region.

Indonesia has not declared the intention to develop explicit cyber clusters. However, they have created what they call "Datavores – data empowered villages"[57] and are in the process of evaluating the impact of these massive data cities. Therefore, they have received a 3 as this is not an explicit cyber cluster, but does show intention to build technology clusters generally.

Philippines received a rank of 3, as the Philippines is currently planning and developing their cyber clusters. This can be seen as the government has taken concrete steps to attract major companies and private investment.

Singapore received a rank of 6 because they have integrated their cyber cluster with their universities.

[56] Margarita Angelidou, "Smart City Strategy: Cyberjaya (Malaysia)."Urenio. http://www.urenio.org/2015/02/09/smart-city-strategy-cyberjaya-malaysia/.

[57] Diastika Rahwidiati and George Hodge. "Imagining a Data Empowered Village." United Nations Global Pulse: Harnessing big data for development and humanitarian action. http://unglobalpulse.org/imagining-data-empowered-village.

Additionally, as a result of state investment and private company investment, their cyber cluster is very capable.

Thailand received a rank of 2 because the government is intending to develop specific and integrated cyber clusters, but has yet to start developing them.

Vietnam received a rank of 2 because they have expressed the intention to build a cyber-cluster in India.

Cyber Militias – The countries were ranked in descending order dependent on the number and quality of their cyber militias. The country with the greatest number of militias, Indonesia, received a 6. The countries with zero cyber militias, Singapore and Vietnam, received ranks of 0.

Formal Education (% Enrollment) – The countries were ranked in descending order dependent on their percentages of enrollment. The country with the highest percentage, Malaysia, received a 6. Both Thailand and Vietnam received a rank of 3. While Vietnam has a lower percentage, as mentioned above in the report, Thailand's enrollment percentage is misleading. The country with the lowest percentage, Indonesia, received a 2, as they do have some success in this field and do not deserve 0.

Formal Education (Number of ABET Accredited Schools) – The countries were ranked in descending order dependent on the number of their universities that have been ABET accredited. Additionally, 0's were awarded to those countries that do not have an ABET Accredited School such as Malaysia and Thailand.

Formal Education (Post-Grad Employment) – The countries were ranked in descending order dependent on their success rate of student post-grad employment. The country with the highest percentage of post-grad employment, Singapore, received a 6. The country with the lowest percentage of post-grad employment, Indonesia, received a 2, as they do have some success in this field and do not deserve 0.

Formal Education (STEM Visa Enrollment %) – The countries were ranked in descending order dependent on their percentage of STEM Visa enrollment. The country with the most STEM Visa Enrollment, Malaysia, received a 6. The country with the least STEM Visa Enrollment, the Philippines, received a 1.

GDP – per capita (PPP) The countries were ranked in descending order dependent on their GDP. The country with the highest GDP, Singapore, received a 6. The country with the least GDP, Vietnam, received a 1.

Hacker Conferences – If a country has hacker conferences, it is likely more cyber threat activity will exist.

Malaysia received a rank of 6 as it boasts a large number of hacking conferences organized in unison with universities and private companies. Additionally, Malaysia also hosts a number international conferences.

Indonesia received a rank of 6, as it boasts an impressive number of hacking conferences and international important gatherings that are focused on the technical aspects of hacking and computer security.

Philippines received a rank of 4 because the country only hosts a few hacking conferences and symposiums on the subject of cyber security.

Singapore received a rank of 5 because of the presence of renowned hacking conferences, mostly organized by universities and research institutes without direct government involvement.

Thailand received a rank of 4, as some hacking conferences exist in the country, but not at the level of the proceeding countries.

Vietnam received a rank of 3 as they have the least amount of hacking conferences of the six examined countries.

Informal Education (Cyber Competitions) – As hacker conferences are normally conducted in tandem with cyber competitions we used the same rationale and rankings as written above for Hacker Conferences.

Informal Education (Hour of Code – Number of Events) – The countries were ranked in descending order dependent on their number of Hour of Code events. The country with the most events, the Philippines, received a 6. The country with the least number of events, Singapore, received a 1.

Informal Education (CompTIA Tech Certification Exam in National Language) – The countries were ranked dependent on whether certifications were available in their primary national language.

Malaysia received a rank of 5 as Malaysia has fully incorporated the CompTIA certifications into its collegiate curriculum, with some courses offering the certification exam as a final exam. While the exam is not offered in Malay, there exists great proliferation of CompTIA interest.

Indonesia received a rank of 3, as there are many classes available in Indonesia to earn this certification, but CompTIA does not currently offer the exam in Indonesian and there is no formal proliferation of the exam within formal education institutions.

Philippines received a rank of 4, as CompTIA certifications are available in English, one of the Philippines' national languages.

Singapore received a rank of 6, as CompTIA certifications are available in English and Chinese, two of Singapore's national languages.

Vietnam received a rank of 3, as there are many classes available in Vietnam to earn this certification, but CompTIA does not currently offer the exam in Vietnamese and there is no formal proliferation of the exam within formal education institutions.

Thailand received a rank of 6, as CompTIA certifications are available in Thai, one of Thailand's national languages.

Informal Education (CISCO Tech Certification Exam in National Language) – The countries were ranked dependent on whether certifications were available in their national language. All countries received a base line score of 3 as we see proliferation of CISCO exam knowledge and there are many institutions that teach CISCO related material. Singapore and the Philippines were boosted to a 4 as CISCO exams are available in English, one of the national languages in these countries, which allows these countries citizens great access as, the exam and study materials are in their native language.

Informal Education (Trade Schools) – All countries received a 6 as the number of trade schools is very high in all six countries.

Informal Education (YouTube Top Provider – Number of Videos) – The countries were ranked in descending order dependent on the number of YouTube videos and overall viewership. The country with the most videos, Singapore, received a 6. The country with the least videos, the Philippines, received a 1.

Malware in National Language – All countries received a base line score of 3 as we see a mastery of hacking from these countries in the English language currently. Singapore, the Philippines, and Thailand were boosted to a rank of 6 as hacks are occurring in their national languages of English and Thai, respectively.

CERT Conduct – If a country has a productive CERT membership, we posit that this membership and activity will reduce cyber threat activity. However, we do recognize that membership to the OIC-CERT may result in more cyber threat activity, as outlined in the report and below.

Malaysia received a rank of 6, as they are a Permanent-Secretariat member of the OIC-CERT.[58] While CERT activity normally deters threat activity, membership to this specific CERT, in tandem with the prospect of religiously motivated hacking, we believe deserved a high threat ranking.

Indonesia received a rank of 3, as they are a member of the OIC-CERT, but do not have high participation rates in the CERT.

[58] "OIC-CERT." OIC-CERT. https://www.oic-cert.org/en/.

Philippines received a rank of 2, as they have a very strong CERT capable of deterring cyber threat activity.

Singapore received a rank of 1, as they have a very strong CERT. Additionally the presence of Interpol diminishes the opportunity to carry out cyber threat activity.

Thailand received a 5, as their lack of CERT coordination allows for cyber threat activity.

Vietnam received a 4, as they have a moderately coordinated CERT, which allows for some cyber threat activity.

Culture – If there exists a culture that allows for or encourages hacker, more cyber threat activity is likely.

Malaysia received a rank of 5, as there is a growing and active community that uses common hacking terms, puts up content online and participates in attacks or supplies offensive talents.

Indonesia received a rank of 6, as there is active, as well as, spreading use of hacking tools and the culture associated with it. The community is active and engaging with outside influences.

Philippines received a rank of 2, as there is a presence of a hacking community but it seems not be very active outside of certain specialized events or an organization.

Singapore received a rank of 5, as there is an active hacking culture developed and supported by government efforts, albeit limited in scope as it is only encouraged at universities.

Thailand received a rank of 3, as there is a hacking culture present in the country but it seems not very connected or active.

Vietnam received a rank of 0 because information on Vietnam was unable to be acquired for this indicator.

Cyber Policy – If a country has a more coordinated cyber policy, they will likely be better able to conduct state-level cyber threat activity, such as espionage against other countries.

Malaysia received a rank of 6, as their coordinated government approach, efficient infrastructure and constant evolution efforts have resulted in strong institutional cyber conduct.

Indonesia received a 4, as their policy is less sophisticated and developing infrastructure remains to be seen as a huge priority for the state.

Philippines received a 5 because they have developed key policies and seek to further develop infrastructure for better intelligence and coordination.

Singapore received a 6, as they have strong policies, and follow through as seen in enforcement and legal structures.

Thailand received a rank of 5 because of coordinated approaches within their enforcement sector.

Vietnam received a 0 because their strategy is less than a year old and is yet to be seen as effective

Cybersecurity Council – If a country has an established cybersecurity council, they will be better able to carry out state-level cyber threat activity.

Malaysia **r**eceived a 6 because of the many informal and formal creations of bodies to advise on cyber issues from the vantage point of education, security, innovation, and financial sectors.

Indonesia received a 0 as they do not have a declared Cybersecurity Council despite discussions of building one.

Philippines received a 6 because they have a Cybersecurity Council. This was largely built in the image of the United States' council.

Singapore received a 6 due to the presence of INTERPOL. With INTERPOL in country, Singapore has a robust and efficient Cybersecurity Council even if it operates under another name.

Thailand received a 0, as it is inconclusive how the Thai government seeks to organize stakeholders into a formal body, such as a Cybersecurity Council.

Vietnam received a 0, as there is no indicator that Vietnam has the intention of developing a Cybersecurity Council.

Declared Cyber Command – If a country has a declared cyber command, they will be better able to carry out state-level cyber threat activity.

Malaysia received a rank of 6, as the 9th Malaysian Development Plan is the liaison to other stakeholders reporting to the Ministry of Science, Technology & Innovation (MOSTI) and effectively serves as Cyber Command.

Indonesia received a 6, as the Ministry of Defence on Cyber Warfare in Military Cyber Indonesian functions as Cyber Command.

Philippines received a 1 in this indicator. While the Philippines has a named CYBERCOM - Armed Forces of the Philippines, this organization has very little information detailing their purpose -- thus, a rating of 1 has been ascribed.

Singapore received a 6, as the SPF Cybercrime Command oversees the Cybercrime Response Team based in every Police Land Division in country.

Thailand received a 0, as there was no found Cyber Command in country.

Vietnam received a 0, as the Chief of Ministry's computer knowledge department, Nguyen Viet The, stated Vietnam needed to prepare for *cyber wars* and urged the country to prepare for the development of a high command in 2011. However, there has been no actual development as a result of this suggestion.

Freedom House Rating – The countries were ranked in descending order dependent on their Freedom House Ranking. The country with the highest Freedom House rating, Indonesia, received a 1, as greater freedom and less oppression in country is likely to result in less cyber threat activity. The country with the lowest Freedom House Rating, Vietnam, received a 6, as a low Freedom House Rating is likely to result in greater cyber threat activity.[59]

Hacking Team Software – A ranking of 6 was awarded to countries that had purchased hacking team software. A ranking of 0 was awarded to countries that had not made this purchase.

Norms – If norms allow for or encourage hacking, there will likely be more cyber threat activity.

Malaysia received a rank of 4 as hacking and insight into IT technology is highly regarded and there is not high condemnation of cyber-crime.

Indonesia received a rank of 4, as hacking and computer science knowledge within the Indonesian environment is highly regarded. Additionally, making money through more illicit means is not particularly condemned either.

Philippines received a rank of 4, as knowledge of computer science, as well as hacking, is seen as a useful skill in the Philippines. Additionally, making money through illicit means is not particularly frowned upon in some of the more remote areas.

Singapore received a rank of 2, as hacking and cybercrime is actively discouraged by government publications and campaigns. Additionally, there are many elements, from high government channels, keeping people from doing illicit types of work.

Thailand received a rank of 4, as hacking and computer-programming skills are highly regarded within the country. There is also not active discouragement of making money by illicit means.

Vietnam received a rank of 2, as computer skills and hacking are seen in a bad light, particularly after the Chinese attacks carried out by APT OceanLotus, as mentioned in Vietnam's country analysis. Another barrier to cyber threat activity is that the Vietnamese

[59] "Freedom in the World: Anxious Dictators, Wavering Democracies: Global Freedom under Pressure." Raw Data. 2016. https://freedomhouse.org/report/freedom-world/freedom-world-2016.

look down upon illicit activities as a means of making money.

Offensive/Defensive – All countries were awarded a base rank of 4 as a defensive posture still allows for state-level cyber threat activity. Thailand was awarded a rank of 6 as they have a declared offensive cyber policy.

Strong Focus on Military – All countries with a stated strong focus, and proven indication of that focus were, awarded a 6. The Philippines does not display this focus and therefore, received a 0.

MOTIVATION INDICATORS:

APT Groups – Countries with an APT, as reported by FireEye, were awarded a rank of 6. Countries without APT activity were awarded a 0.

Blocked Access – All six examined countries block access, which creates incentive for hacking. Therefore, all six countries were awarded a rank of 6.

Curiosity – If curiosity of hacking and technology is encouraged, there will likely be more cyber threat activity.

Malaysia received a rank of 5, as hacking, coding and programming are actively encouraged subjects both by government and private company initiatives.

Indonesia received a rank of 5, as hacking, coding and programming is actively encouraged an accompanied by government support at many technical universities.

Philippines received a rank of 5, as coding, programming are highly encouraged by recruiting companies and universities that attempt to export a coding-capable workforce to the US.

Singapore received a rank of 4, as hacking is not encouraged outside of very limited government spaces and controlled university initiatives.

Thailand received a rank of 1, as the government heavily discourages curiosity into hacking and universities do not feature a lot of initiatives to promote curiosity.

Vietnam received a rank of 0, as our research did not yield any results regarding curiosity within the country.

Domestic Politics – If domestic politics are highly contested, citizens may be motivated to carry out cyber threat activity against their governments.

Malaysia received a rank of 3, as there is some contestation in the country. However, Malaysia still remains stable and well governed. Recently revelations over major government corruption have caused a nation-wide uproar, which, resulted in an increased rank of 3.

Indonesia received a rank of 3, as domestic politics have some contestation especially between religious motivated actors and non-religious motivated actors. There is also tension regarding inequality of infrastructure investments that only benefit rich regions. Additionally, we also observed moderate corruption in Indonesia.

Philippines received a rank of 5, as domestic politics is highly contested with indiscriminate killings, corruption and rebels in the south of the country.

Singapore received a rank of 4 because of the harsh laws on public speaking, large inequality and some corruption cases that have made politics more contested.

Thailand received a rank of 5 because the recent coup, differences between regions, and overall inequality in the country have made domestic politics a highly contested subject.

Vietnam received a rank of 4 because rising inequality, high unemployment and a more repressive government has created a state with moderately contested politics.

Geopolitics – If there is conflict with other countries, citizens may feel inclined to hack on behalf of their country.

Malaysia received a rank of 4 because of the tense situation in the South China Sea, and some border

conflicts with immediate neighbors, especially Indonesia

Indonesia received a rank of 4 because of tense situations in the South China Sea, difficult relations with East Timor, and sometimes tense relations with Malaysia.

Philippines received a rank of 6 because of the tense situation in the South China Sea, border conflicts and direct clashes with China over sovereignty issues.

Singapore received a rank of 2 as they have no major international conflicts and serve as a neutral business hub of the region. However, it is important to note that Singapore does have some minor issues with ASEAN and China on the South China Sea.

Thailand received a rank of 4, as they have a few minor border disputes with neighboring countries, but are not directly involved in the South China Sea dispute.

Vietnam received a rank of 5, as they have a large conflict with China over sovereignty in the South China Sea that have already led to cyber-attacks.

Inequality in Income – We used the SWIID Rank to determine inequality income. A low SWIID score indicates high inequality. Therefore, the country with the lowest SWIID score. Indonesia, received a 6, as inequality breed motivation and thus, cyber threat activity. The country with the highest SWIID Rank, Thailand, received a 1, as equality breeds less motivation for cyber threat activity.

Patriotism/Hacktivism – This indicator was a quantitative indicator, but does require further expansion. Therefore, we have provided specific justification for each country's ranking, in order of highest cyber threat activity score to lowest cyber threat activity score, below.

Malaysia received a rank of 6, as there are numerous attacks carried out by Malaysian citizens. Directed at their government, over privacy and surveillance issues as well as patriotic hacking attributed to actors acting on behalf of Malaysian desired outcomes against targets in Singapore and Indonesia.

Indonesia received a rank of 6, as there are numerous patriotic and hacktivist attacks that have targeted the Indonesian government over internet freedom issues, as well as attacks on behalf of Indonesia against targets that are perceived to have insulted the nation.

Philippines received a rank of 6, as there are a high number of previous attacks that have been aligning with hacktivist goals. Additionally, Anonymous Philippines is very active against the new government. Patriotic hacking against China, Indonesia and other countries in the region has also been observed.

Singapore received a rank of 4 because of the lack in patriotic hacking on behalf of Singapore. However, some hacktivist activity including a Singapore Anonymous hacker collective, that targeted the Singapore government's freedom of expression rules and cyber security laws.

Thailand received a rank of 6, as we observed patriotic hacking conducted by Thai hacker groups aimed at attacking Cambodian computers. Their aim was to deface and attack websites. Additionally, hacktivists have targeted the Thai government over social surveillance issues and cyber security laws.

Vietnam received a rank of 3, as there is some patriotic hacking reported especially against Chinese targets, but there is not much hacktivism activity reported.

Previous Attacks – Using FireEye's research on previous attacks and other sources, we were able to determine a ranking for each country. The countries were ranked in descending order dependent on the number and sophistication of attacks. The countries with the highest number of attacks, the Philippines and Thailand, received a 6. The countries with the lowest number of attacks, Indonesia and Vietnam, were awarded a rank of 4.

Pride/Ego – This indicator was a quantitative indicator, but does require further expansion. Therefore, we have provided specific justification for each country's ranking, in order of highest cyber threat activity score to lowest cyber threat activity score, below.

Malaysia received a rank of 5, as hacker groups in the Malaysian community notify and announce attacks in addition to actively challenging other communities. It can be seen that Malaysian hackers take great pride in their work and efforts.

Indonesia received a rank of 4 because pride of the Indonesian hacking groups is moderately high and these groups are actively putting out newsletters, announcements and reports of their attacks.

Philippines received a rank of 4, as parts of the hacking community are somewhat active in attacks, reporting and boasting about their attacks online.

Singapore received a rank of 5, as some hackers or hacking groups have actively boasted and announced their attacks on the government before striking. These announcements were made as an effort to garner attention and build reputation.

Thailand received a rank of 3, as hacking groups are usually not as outspoken or boastful. Thai hacktivists even usually conduct attacks anonymously.

Vietnam received a rank of 4 because of some groups be it hacktivist or patriotic hacking groups are actively reporting and publicly discussing their attacks.

Religion – If a country defines itself by a certain religious ideology or has a very high number of religious individuals, cyber threat activity may occur, as religious motivated hacking may be directed at other religions.

Malaysia received a rank of 6, as they have a high number of Islamic citizens.

Indonesia received a rank of 6, as they have a high number of Islamic citizens.

Philippines received a rank of 6, as they have a high number of Roman-Catholic citizens.

Singapore received a rank of 0, as they do not have a national state religious based identity.

Thailand received a rank of 0, as they do not have a national state religious based identity.

Vietnam received a rank of 0, as they do not have a national state religious based identity.

Screen Time – The countries were ranked in descending order dependent on their number of screen time hours. The countries with the most screen time, Singapore and Vietnam, received a 6. The four other countries recorded 6 hours per day of screen time and thus, received a 5.

Spying – Spying closely aligned with geopolitics. Therefore, we used the same rationale as written for geopolitics to award rankings for this indicator.

Unemployment Rate – The countries were ranked in descending order dependent on their unemployment rate. The country with the highest unemployment, the Philippines, received a 6. The country with the lowest unemployment rate, Thailand, received a one.

Website Defacements – The countries were ranked in descending order dependent on their number of website defacements. The country with the most defacements, Thailand, received a 6. The country with the lowest number of defacements, Singapore, received a one.

Youth Unemployment Rate – The countries were ranked in descending order dependent on their youth unemployment rate. The country with the highest youth unemployment, Indonesia, received a 6. The country with the lowest youth unemployment rate, Thailand, received a one.

OPPORTUNITY INDICATORS:

Budapest Convention – None of the examined countries have signed or ratified the Budapest Convention.[60] As such, they all received a rank of 6. Malaysia has instituted laws that align with the Budapest Convention and therefore, received a 5.

[60] "Details of Treaty No. 185 Convention on Cybercrime." Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Cyber Crime Arrests/Indictments – Countries with the lowest number of arrests were awarded the highest cyber threat activity score, as lax laws allow for great opportunity to hack. Therefore, the country with the lowest number of arrests, the Philippines, received a 6. The country with the highest number of arrests, Thailand, received a 1.

Cyber Enforcement – Countries with good cyber enforcement were awarded a low cyber threat activity score, as enforcement reduces opportunity. Therefore, the country with the great enforcement, Thailand was awarded a 1. The countries with the least enforcement, the Philippines and Vietnam, were awarded a 5.

Cyber Law – Countries with existing cyber laws, received a low ranking in this indicator, as the existence of law serve as an opportunity barrier. Those with less or no cyber laws received a higher cyber threat activity score. Therefore, the countries with the least cyber laws, Indonesia and the Philippines, received a 4. The countries with the most cyber law, Malaysia, received a 1.

Informal Economy (Black Market) – Measuring the size of the informal economy we awarded high ranking to those countries with larger informal economies. Therefore, Indonesia and the Philippines, countries that have large informal economies, received rankings of 6. Conversely, Singapore, a country with a small informal economy, received a 1.

Non-Align Movement – All countries are members of the non-align movement. Therefore, all countries received a rank of 6 as non-alignment indicates an unwillingness to align with Western cyber norms.

UN Group of Experts – As all countries are member of the non-align movement and disregard norms created by the UN Group of Experts, we awarded all countries a base score of 6. However, Malaysia is one the UN Group of Experts member countries. Therefore, we have awarded them a 5.

GENDER INDICATORS:

Gender Development Index – A low GDI score indicates more gender inequality. Therefore, the country with the lowest GDI score, Indonesia, received a ranking of 6, as inequality breeds motivation to conduct cyber threat activity. Vietnam received a rank of 1 as they have the highest GDI score, indicating greater equality.

Gender Inequality Index – As a low gender inequality score signals more equality, countries with a low inequality score were awarded a low rank. Therefore, Malaysia, the country with the lowest Gender Inequality Index score, received a 1. Conversely, Singapore received a rank of 6, as they had the highest GII score.

Population with some secondary education, male – The countries were ranked in descending order dependent on their percentage of males with secondary education. The country with the highest percentage, Singapore, received a 6. The country with the lowest percentage, Thailand, received a one.

Population with some secondary education, female – The countries were ranked in descending order dependent on their percentage of females with secondary education. The country with the highest percentage, Singapore, received a 6. The country with the lowest percentage, Thailand, received a one.

INVESTMENT INDICATORS:

Investment – If a country is investing in the future growth of capability within its country, in terms of capacity, this may indicate a growth of cyber threat activity in the future

Malaysia received a rank of 6 in investment. Malaysia's strength comes from their superior ability to match citizens with jobs. This investment in the people aspect of cyber earned them a rank of 6. While Malaysia is troubled with stimulus fund mismanagement and corruption, as outlined in the country analysis, we believe this is overshadowed by their investment in the Malaysian citizenry for this indicator.

Indonesia received a rank of 5 in investment. While Indonesia has the largest economy of the six nations, they are bad at matching their citizenry with needed job. This lack of alignment stops their investments from achieving their full potential.

Philippines received a rank of 6 in investment. The Philippines is the world fastest growing economy. Additionally, the government channels and promotes investments in the cyber security and IT sectors.

Singapore received a rank of 6, as the Singaporean economy is small, well organized and easily controlled. Matching investment to economic needs occurs with great efficiency in Singapore, as well as focusing investment in the cyber security and IT sectors.

Thailand received a rank of 4 in investment. Thailand's economy is seen as an attractive place to invest tourist dollars. However, tourism has not proven to be a sufficient resource for cyber development. Thailand is not overly focused on cyber or cyber infrastructure, as can be seen by the general lack of cyber funding and investment.

Vietnam received a rank of 4 in investment. While Vietnam receives a lot of investment from within the region, international investment remains low. While Vietnam is missing investment opportunities from the West, they have engaged with India and we may begin to see investment into Vietnam from India, but this is unclear currently.

10. Glossary

Access to Electricity (% of population): Access to electricity is the percentage of population with access to electricity. Electrification data are collected from industry, national surveys and international sources.[61]

Adult Literacy Rate (% ages 15 and older): Percentage of the population age 15 and above who can, with understanding, read and write a short, simple statement on their everyday life. Generally, 'literacy' also encompasses 'numeracy', the ability to make simple arithmetic calculations. This indicator is calculated by dividing the number of literates aged 15 years and over by the corresponding age group population and multiplying the result by 100.[62]

APT Groups: Existence and Activity of APT groups either from the respective country or activity of APT groups within the country as a target. Both instances are driving up the cyber threat level and are important to be factored into our analysis.

Bandwidth Production: This is a measure of domestic bandwidth production. Bandwidth is the width of the 'pipe' through which data travels: greater the width, larger the amount of data that can flow through it. As bandwidth grows, more data can be transferred allowing for better Internet access.[63]

Blocked Access: This indicator measures the government's ability to block access to sites and unwanted content. This includes both the government's ability to control access to content, which may provoke citizens to circumvent blocked access through technological means (VPN, specialty browsers etc.)

Budapest Convention: The Budapest Convention was the first international treaty, signed by the Council of Europe in 2001, seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. A country that has signed and ratified this treaty will likely see less cyber threat activity as there is clear and unified enforcement against such activity.

CERT Conduct: A CERT is a Computer Emergency Response Team. These teams respond in times of crisis, such as when a hack occurs. The activity level and conduct of a country's CERT was measured in this indicator. A very active CERT is a good indicator for overall government capability in the sector and may result in less cyber threat activity.

Culture: The existence or lack of a hacker culture in country can encourage or discourage behavior. The presence of a hacking culture may drive up cyber threat activity, as people are encouraged by the example and knowledge of others that are seen as role models.

[61] Definition retrieved from the World Bank. See Works Cited.
[62] Definition retrieved from the World Bank. See Works Cited.
[63] Definition retrieved from Packet Clearing House. See Works Cited.

Curiosity: Curiosity is the measure of how a government or culture encourages its citizens to be curious about technology.

Cyber Clusters: Cyber clusters are dedicated areas where research, business and state entities cooperate to create synergy effects. Willingness to establish cyber clusters highlights cyber focus and the potential for greater cyber capability within a country.

Cyber Crime/Arrests/Indictments: While countries may have very strict cyber laws on the books, the enforcement of those laws may not align with what's on paper. To gain real insight into how a country enforces its laws, we examined cyber arrests. Cyber arrests show how policy is enforced and how much of a deterrent is created through such arrests.

Cyber Enforcement: This metric measures the overall culture behind enforcement in a country. Similar to the culture indicator, a permissive attitude toward cybercrime from government officials may play a role in increasing cyber threat activity.

Cyber Law: The existence of specific cyber laws and regulations that would deter actors from breaking into computers and physical systems of the Internet. This indicator is valued as a deterrent. The existence of specific laws shows determination and technological knowledge in order to enforce against malicious actors.

Cyber Militias: Active Groups attempting to act on behalf of their nation state in regards to religious or cultural matters. The existence of these groups shows a common culture and a common path towards influencing nation states. The more groups a country has active in its borders, the more likely cyber threat activity becomes.

Cyber Policy: The existence of a coherent and actionable cyber policy that conveys clear intention on the side of the government. This policy can reach beyond the cyber security field and include ambitions for education, infrastructure and research.

Cyber Power: Defines the full extent of state ability in cyberspace. Aiming at all levels of national power be it administrative, military or human resources that can be used to project national influence onto cyberspace.

Cybersecurity Council: The existence of a clear coherent council that manages and regulates the cyber security field from a whole-of-government approach. Elevating cyber security to a higher level of scrutiny and government attention (and spending).

Declared Cyber Command: The existence of a military command signals the understanding of cyberspace as a strategic domain, which speaks to the capabilities and resources dedicated to the new domain within a country.

Domestic Politics: The state of domestic politics may increase cyber threat levels. Broadly speaking, insecurity, weak cohesion in government politics, the existence of rebel groups and the general conduct of politics will either increase or decrease cyber threat activity. The domestic politics indicator is placed within the motivation sector, as it is one of the main drivers that motivates cyber threat activity. In essence, actors will use their hacking abilities to attempt to disrupt domestic politics they perceive as hostile or unjust.

Fixed Broadband Subscriptions (per 100 people): Fixed broadband subscriptions refer to fixed subscriptions to high-speed access to the public Internet (a TCP/IP connection), at downstream speeds equal to, or greater than, 256 kbit/s. This includes cable modem, DSL, fiber-to-the-home/building, other fixed (wired)-broadband subscriptions, satellite broadband and terrestrial fixed wireless broadband. This total is measured irrespective of the method of payment. It excludes subscriptions that have access to data communications (including the Internet) via mobile-cellular networks. It should include fixed WiMAX and any other fixed wireless technologies. It includes both residential subscriptions and subscriptions for organizations.[64]

[64] Definition retrieved from the World Bank. See Works Cited.

Formal Education (Enrollment): The number of students enrolled in formal computer science programs at the undergraduate, master's or PhD level. A higher number of students means a larger talent pool and potentially more people with an understanding of computer science and related coding knowledge.

Formal Education (Number of ABET Accredited Schools): ABET accredits college and university programs in the disciplines of applied science, computing, engineering and engineering technology at the associate, bachelor and master degree levels. ABET Accreditation shows that a country is adhering to international standard of STEM education. The more ABET accredited schools in a country, the more likely it is that capacity will grow and thus, potentially cyber threat activity.[65]

Formal Education (Post-grad Employment): Employment percentage totals for graduating students. The statistics do not measure graduation in related fields but rather overall, which is still a good indicator for general implications of employment highly qualified individuals within a country.

Formal Education (STEM Visa Enrollment %): Number of people from the six countries that apply for a STEM visa to study in the United States. This shows how many talented people in the fields are coming from each country giving further definition to the potential talent pool.

Freedom House Rating: Freedom House ratings measure a range of different vectors such as press freedom, economic participation, enforcement of laws. etc. A country's Freedom House rating offers a good indication of the level of freedom citizens have. This ranking speaks to a general level of repression that may incentivize cyber threat actors to conduct malicious activity.

GDP Per Capita (PPP): Basic measurement of wealth of a country and an indicator for general standards. Countries with a higher GDP will likely exhibit more *capability*.

Gender Development Index: Ratio of female to male HDI values. A higher value shows more inequality between males and females.[66]

Gender Inequality Index: A composite measure reflecting inequality in achievement between women and men in three dimensions: reproductive health, empowerment and the labor market. The higher the number the more gender inequality exists within a country.[67]

Geopolitics: The geopolitical situation in a country may be a deterrent to or a driving factor of malicious activity. A tense geopolitical situation or an environment of hostility may motivate patriotic hacktivism and state action as a way to retain an advantage over other states. As such, a tenser geopolitical situation opens the door for higher cyber threat activity.

Hacker Conferences: Hacker conferences highlight the proliferation, acceptance, and community of hacking within a country. A country with highly attended and frequent hack conferences will likely exhibit more cyber threat activity.

Hacking Team Software Usage: The recent data leaks of hacking team software have revealed a number of countries buying their technology and being consulted on technology and cyber security processes. The use and application of this software speaks to a certain maturity and intention to user cyber espionage in law enforcement or even domestic surveillance.

Inequality in Income: The Standardized World Income Inequality Database, SWIID, rank measures the trends of (a) inequality in net (post-tax, post-transfer) income, (b) inequality in market (pre-tax, pre-transfer) income, (c) absolute redistribution (market-income inequality minus net-income inequality), or (d) relative redistribution (market-income inequality minus net-income inequality, divided by market-income inequality) Using this, we were able to rank the countries. A country with more inequality is likely to have a citizenry that is more likely to hack.[68]

[65] Definition retrieved from the official ABET website. See Works Cited.
[66] Definition retrieved from the United Nation Human Development Report. See Works Cited.
[67] Definition retrieved from the United Nation Human Development Report. See Works Cited.
[68] Definition retrieved from the website of Frederick Solt, the develop of the

Informal Economy (Black Market): A crucial indicator for execution and durability of cyber threat activity. The size and organization of black market activity is crucial for actors that want to launder money gained from malicious cyber activity, recruit offensive cyber talent and/ or aim to establish a network for stolen goods. In general, the informal economy provides several opportunities to malicious actors and is an important part of cyber threat activity. As such, the bigger and more sophisticated the black market, the higher the cyber threat activity.

Informal Education (CISCO Tech Certification Exam in National Language): Whether or not CISCO exams are available in the country's national language. Cyber certifications are a globally recognized metric of cyber aptitude.

Informal Education (CompTIA Tech Certification Exam in National Language): Whether or not CompTIA exams are available in the country's national language. Cyber certifications are a globally recognized metric of cyber aptitude.

Informal Education (Cyber Competitions): The existence of cyber competitions within a country highlights the path that those who are informally educated may take in becoming hackers. Cyber competitions convey that a country is thinking about cyber issues, policies, hacking, and technologies. This conveys a more capable citizenry. Thus, a high number of cyber competitions will likely result in greater cyber threat activity.

Informal Education (Hour of Code - Number of Events): The Hour of Code started as a one-hour introduction to computer science, designed to demystify "code", to show that anybody can learn the basics, and to broaden participation in the field of computer science. It has since become a worldwide effort to celebrate computer science, starting with 1-hour coding activities but expanding to all sorts of community efforts. A country with more hours of code will likely have a population that is more familiar with computers. Thus, more hours of code build capacity and may likely contribute to cyber threat activity.[69]

Informal Education (Trade Schools): Trade schools are a common path of informal education to gain computer skills. This indicator measures whether or not trade schools teaching coding are available in the national language of a country. Additionally, the types of training were examined. A country with more types of training available in its language will likely display more cyber threat activity.

Informal Education (YouTube Top Provider - Number of Videos): The prevalence of YouTube videos by formal companies within a country, in the national language, conveys a strong path for informal education.

Internet Servers Using Encryption: Secure servers are servers using encryption technology in Internet transactions. The more servers using encryption, the greater the likelihood for cyber threat activity, as the use of encryption indicates greater capability. Fully encrypting web-traffic requires moderate knowledge of technology.

Internet Users (per 100 people): Internet users are individuals who have used the Internet (from any location) in the last 12 months. The Internet can be used via a computer, mobile phone, personal digital assistant, games machine, digital TV etc. The higher the number of people using the Internet, the more likely cyber threat activity becomes.[70]

Investment: Investment indicates potential future growth of a country's citizens in terms of education investment or a country's infrastructure in terms of infrastructure investment. Investment indicates government commitment. We rank countries according to their ongoing investment in the area (public or private) and consider how the state response to allowing businesses and new technologies to develop markets and/or transform new systems to be more efficient.

SWIIF Database. See Works Cited.

[69] Definition retrieved from the Hour of Code Website. See Works Cited.

[70] Definition retrieved from the World Bank. See Works Cited.

IXP: An IXP is the physical infrastructure, through which Internet traffic is exchanged. Having 1 IXP allows a country to control its domestic Internet and not rely on another country's IXP. With more IXP's, a country can exchange more data.

Malware In National Language: Existence of malware that is written or spread in national language or might contain certain keywords/phrases that have their origin in a national language.

Non-Align Movement (Member): The Non-Align Movement positions countries to not-align with any Western or major superpowers. This shows a disregard for the great cyber powers and overall discontent with the international hierarchy system. A country participating in the Non-Align Movement will likely have more cyber threat activity as a retaliation against Western values, impositions and orders.

Norms: Norms were measured as either permissive, indifferent or deterrent to cyber threat activity. An admiration for hacking within a country or a constructed norm that hacking is okay may allow for greater cyber threat activity.

Number of ISPs: The number of Internet Service Providers in a country. Having more service providers often allows for better access.

Offensive/Defensive: Cyber security policy declared as offensive or defensive. This can be used as a measure of state aggressiveness. A state with an offensive policy may be more aggressive and will likely pose a larger cyber threat domestically and internationally.

Patriotism/Hacktivism: The occurrence and prevalence of a hacktivist groups and the presence of patriotic specific hacking. Citizens may be motivated to act on behalf of internet freedoms, the Anonymous collective or on behalf of their nation.

Population with at least some secondary education, female (% ages 25 and older): Percentage of the population ages 25 and older that has reached (but not necessarily completed) a secondary level of education. The higher the percentage, the more female citizens have attained some secondary education.[71]

Population with at least some secondary education, male (% ages 25 and older): Percentage of the population ages 25 and older that has reached (but not necessarily completed) a secondary level of education. The higher the percentage, the more male citizens have attained some secondary education.[72]

Previous Attacks: Measures previous attacks on systems, companies, government websites and other internet technology related infrastructure. A high level of past cyber threat activity may be indicative of a higher cyber threat activity level.

Pride/Ego: Cyber talented individuals may be motivated by financial gain or patriotic reasons. However, they may also be motivated by pride or ego. These individuals hack because they want to display their technological and coding prowess.

Religion: Religiously motivated hacking measures the root cause of specific hacker attacks. Our research has shown evidence that some malicious activity coming from countries in the region has a distinct religious motivation. Countries are ranked according to how much religion may drive malicious activity.

Screen Time (Number of Hours/Day/Person): Hours spent daily on computer screens (Smartphone, Laptop, Desktop, TV, All Screens). While this measure encompasses many different types of screens, screen time is still fundamentally important to hacking. Familiarity with a computer can be seen within this measure. More hours in front a screen denote a higher level for indirect threat activity.

Spying: The prevalence of cyber espionage either targeting companies, private data, individuals or even government entities is a good level of indication for high cyber threat activity.

Strong Focus on Military: The existence of a strong focus on the national military highlights state

[71] Definition retrieved from the United Nation Human Development Report. See Works Cited.

[72] Definition retrieved from the United Nation Human Development Report. See Works Cited.

likelihood for aggression. A stronger focus on military in the 21st century normally includes a focus on cyber capabilities and development. As such, states with a strong focus on military will likely pose a larger cyber security threat.

UN Group of Experts (Member): The UN Group of Experts convenes to create international cyber norms. Participation in the UN Group of Experts shows great skill and willingness to participate in the international system. A member country will likely be less likely to display cyber threat activity, as a participating member sets norms against such activity.

Unemployment Rate (% of Labor Force): Percentage of the labor force population ages 15 and older that is not in paid employment or self-employed but is available for work and has taken steps to seek paid employment or self-employment. Higher levels of unemployment are likely to cause citizens to explore other avenues of employment, income, or use of idle time, such as hacking.[73]

Website Defacements: Website defacements measures how many websites are defaced within a country in a given year, 2013. The more websites defaced, the more cyber threat activity is occurring.

Youth Unemployment Rate (% of Labor Force Ages 15-24): Percentage of the labor force population ages 15-24 that is not in paid employment or self-employed but is available for work and has taken steps to seek paid employment or self-employment. Higher levels of unemployment are likely to cause young citizens to explore other avenues of employment, income, or use of idle time, such as hacking.[74]

[73] Definition retrieved from the United Nation Human Development Report. See Works Cited.

[74] Definition retrieved from the United Nation Human Development Report. See Works Cited.

11. Appendix

Indicator	Year	Indonesia	Malaysia	Phillipines	Singapore	Thailand	Vietnam	Total Weight	Time Span	Defintion	Source
Capability											
Connectivity											
Access To Electricity (% of populatic	2012	96	100	87.5	100	100	99	high/direct	short	Access to electri	All Countries: htt
Bandwidth Production	2016	16.1G	838M	11.6G	378G	3.25G	12.3G	low/direct	short	This is a measur	All Countries: htt
Bandwidth Production	2017	101G	838M	18G	724G	13.4G	24.7G	low/direct	short	This is a measur	All Countries: htt
Fixed Broadband Subscriptions (per	2015	1.09	8.95	3.4	26.45	9.24	8.14	medium/indirect	short	Fixed broadband	All Countries: htt
Internet Servers Using Encryption	2015	2,050	3,148	1,378	5,159	2,067	1,353	medium/indirect	short	Secure servers a	All Countries: htt
Internet Users (per 100 people)	2015	22	71.1	40.7	82.1	39.3	52.7	high/direct	short	Internet users ar	All Countries: htt
IXP	2016	6	1	1	4	2	3	low/indirect	short	An IXP is the phy	All Countries: htt
IXP	2017	7	1	1	5	2	3	low/indirect	short	An IXP is the phy	All Countries: htt
Number of ISPs	2003	24	7	3	9	15	5	low/direct	short	The number of In	All Countries: htt
Capacity											
Adult Literacy Rate (% ages 15 and	2015	95	95	97	97	94	95	high/direct	short/long	Percentage of th	All Countries: htt
Cyber Clusters	---	---	---	---	---	---	---	medium/indirect	short/long	The existence an	---
Cyber Militias (Number of Militas)	---	10	3	4	0	2	0	high/indirect	short	Active Groups at	Indonesia: http://j
Formal Education (% Enrollment)	---	11	23.5	20	18	19	12.5	high/indirect	short/long	Number of stude	---
Formal Education (Number of ABET	2016	4	0	4	2	0	1	high/indirect	short/long	ABET accredits c	All Countries: htt
Formal Education (Post-grad Emplo	---	---	---	---	---	---	---	high/indirect	short/long	General employn	---
Formal Education (STEM Visa Enro	2014	29.7	53.7	19.8	27.9	25.6	26.5	high/indirect	short/long	Number of peopl	All Countries: htt
GDP - per capita (PPP)	2016	11,700	27,200	7,700	87,100	16,800	6,400	medium/indirect	short/long	Basic measurem	All Countries: htt
Hacker Conferences	---	yes	yes	yes	yes	yes	yes	high/indirect	short/long	Hacker conferen	All Countries: htt
Informal Education (Cyber Competit	---	yes	yes	yes	yes	yes	yes	high/direct	long	The existence of	All Countries: htt
Informal Education (Hour of Code - I	2017	332	118	811	62	114	155	high/direct	long	The Hour of Cod	All Countries: htt
Informal Education (CompTIA Tech	---	no	no	yes (English)	yes (English/Chir	yes (Thai)	no	medium/direct	long	CompTIA exams	All Countries: htt
Informal Education (CISCO Tech Ce	---	no	no	yes (English)	yes (English)	no	no	medium/direct	long	CISCO exams av	All Countries: htt
Informal Education (Trade Schools)	---	---	---	---	---	---	---	high/direct	long	Trade schools ar	---
Informal Education (Youtube Top Pr	2017	567	369	12	2,697	337	428	medium/direct	long	The prevalence c	Indonesia: https:/
Malware in National Language	---	---	yes (Malay)	yes (English)	yes (English/Mal	yes (Thai)	---	medium/direct	short/long	Existence of mal	---
Conduct											
CERT Conduct	---	---	---	---	---	---	---	medium/indirect	short	Activity level and	---
Culture	---	---	---	---	---	---	---	high/indirect	short/long	The existence of	---
Cyber Policy	---	---	---	---	---	---	---	medium/indirect	short/long	The existence of	---
Cybersecurity Council	---	---	---	---	---	---	---	low/indirect	short/long	The existence of	---
Declared Cyber Command	---	---	---	---	---	---	---	low/indirect	short/long	The existence of	---
Freedom House Rating	2017	65	44	63	51	32	20	low/indirect	short	General rank of f	All Countries: htt
Hacking Team Software	---	---	---	---	---	---	---	medium/indirect	short/long	The recent data l	---
Norms	---	---	---	---	---	---	---	high/indirect	short/long	Norms that are e	---
Offensive/Defensive	---	defensive	defensive	defensive	defensive	offensive	defensive	high/indirect	short/long	Cyber security pc	Indonesia: https:/
Strong Focus on Military	---	---	---	---	---	---	---	high/direct	short/long	The existence of	---
Motivation											
APT Groups	---	---	---	---	---	---	---	high/indirect	short	Existence and Ac	---
Blocked Access	---	yes	yes	yes	yes	yes	yes	medium/indirect	short	This vector mean	Indonesia: https:/
Curiousity	---	---	---	---	---	---	---	medium/direct	short/long	Curiosity is the m	---
Domestic Politics	---	---	---	---	---	---	---	high/direct	short/long	The state of dom	---
Geopolitics	---	---	---	---	---	---	---	high/direct	short/long	The geopolitical s	---
Inequality in Income (1 = high inequ	---	1	4	2	3	6	5	high/direct	short/long	The SWIID RANI	All Countries: htt
Patriotism/Hacktivism	---	---	---	---	---	---	---	high/direct	short/long	The occurrence a	---
Previous Attacks	---	---	---	---	---	---	---	high/indirect	short	A good indicator	---
Pride/Ego	---	---	---	---	---	---	---	high/indirect	short	There are some c	---
Religion	---	---	---	---	---	---	---	medium/direct	short/long	Religiously motiv	---
Screen Time (Number of Hours/Day	2014	6	6	6	8	6	8	low/indirect	short	Hours spent daily	All Countries: htt
Spying	---	---	---	---	---	---	---	high/direct	short/long	The prevalence c	---
Unemployment Rate (% of Labor Fo	2015	5.8	2.9	6.7	3.3	1.1	2.1	high/direct	short/long	Percentage of th	All Countries: htt

Indicator	Year	Indonesia	Malaysia	Phillipines	Singapore	Thailand	Vietnam	Total Weight	Time Span	Defintion	Source
Website Defacements	2013	3,500	2,250	500	800	4,300	3,100	high/indirect	short	Website defacem	All Countries: htt
Youth Unemployment Rate (% of La	2015	19.3	10.4	15.7	7.3	4.7	5.3	high/direct	short/long	Percentage of th	All Countries: htt
Opportunity											
Budapest Convention (Signed/Ratifi	---	no	no	no	no	no	no	low/indirect	short	The Budapest Co	All Countries: htt
Cyber Crime Arrests/Indictments	---	---	---	---	---	---	---	high/direct	short/long	While countries r	---
Cyber Enforcement	---	---	---	---	---	---	---	high/direct	short/long	This metric meas	---
Cyber Law	---	---	---	---	---	---	---	medium/indirect	short/long	The existence of	---
Informal Economy (Black Market)	---	---	---	---	---	---	---	high/direct	short/long	A crucial indicato	---
Non-Align Movement (Member)	---	yes	yes	yes	yes	yes	yes	low/indirect	short	The Non-Align M	All Countries: htt
UN Group of Experts (Member)	---	no	yes	no	no	no	no	low/indirect	short	The UN Group of	All Countries: htt
Gender											
Gender Development Index	2014	0.928	0.935	1	0.984	1.001	1.008	low/indirect	short/long	Ratio of female t	All Countries: htt
Gender Inequality Index	2015	0.467	0.291	0.436	0.068	0.366	0.337	medium/direct	short/long	A composite mea	All Countries: htt
Population with at least some secon	2015	51.7	79.1	70.3	81.9	45.8	76.7	medium/indirect	short/long	Percentage of th	All Countries: htt
Population with at least some secon	2015	42.9	75.4	72.8	75.5	40.9	64	medium/indirect	short/long	Percentage of th	All Countries: htt
Investment											
Investment	---	---	---	---	---	---	---	high/direct	short/long	Investment is a u	All Countries: htt

Raw Data

Calculations

Indicator	Year	Indonesia	Malaysia	Phillipines	Singapore	Thailand	Vietnam	Total Weight	Total Weight #	Minumum	Maximum	Indonesia Total	Malaysia Total	Phillipines Tota	Singapore Total	Thailand Total	Vietnam Total
Capability																	
Connectivity																	
Access To Electricity (% of popula	2012	5	6	4	6	6	6	high/direct	6	0	36	30	36	24	36	36	36
Bandwidth Production	2016	5	1	3	6	2	4	low/direct	2	0	12	10	2	6	12	4	8
Bandwidth Production	2017	5	1	3	6	2	4	low/direct	2	0	12	10	2	6	12	4	8
Fixed Broadband Subscriptions (p	2015	1	4	2	6	5	3	medium/indirect	3	0	18	3	12	6	18	15	9
Internet Servers Using Encryption	2015	3	5	2	6	4	1	medium/indirect	3	0	18	9	15	6	18	12	3
Internet Users (per 100 people)	2015	1	5	3	6	2	4	high/direct	6	0	36	6	30	18	36	12	24
IXP	2016	6	2	2	5	3	4	low/indirect	1	0	6	6	2	2	5	3	4
IXP	2017	6	2	2	5	3	4	low/indirect	1	0	6	6	2	2	5	3	4
Number of ISPs	2003	6	3	1	4	5	2	low/direct	2	0	12	12	6	2	8	10	4
Capacity																	
Adult Literacy Rate (% ages 15 an	2015	5	5	5	5	5	5	high/direct	6	0	36	30	30	30	30	30	30
Cyber Clusters	---	3	6	3	6	2	2	medium/indirect	3	0	18	9	18	9	18	6	6
Cyber Militias (Number of Militas)	---	6	3	5	0	4	0	high/indirect	5	0	30	30	15	25	0	20	0
Formal Education (% Enrollment)	---	2	6	5	4	3	3	high/indirect	5	0	30	10	30	25	20	15	15
Formal Education (Number of ABE	2016	6	0	6	5	0	4	high/indirect	5	0	30	30	0	30	25	0	20
Formal Education (Post-grad Empl	---	2	5	4	6	3	3	high/indirect	5	0	30	10	25	20	30	15	15
Formal Education (STEM Visa Enr	2014	5	6	1	4	2	3	high/indirect	5	0	30	25	30	5	20	10	15
GDP - per capita (PPP)	2016	3	5	2	6	4	1	medium/indirect	3	0	18	9	15	6	18	12	3
Hacker Conferences	---	6	6	4	5	4	3	high/direct	5	0	30	30	30	20	25	20	15
Informal Education (Cyber Compet	---	6	6	4	5	4	3	high/direct	6	0	36	36	36	24	30	24	18
Informal Education (Hour of Code	2017	5	3	6	1	2	4	high/direct	6	0	36	30	18	36	6	12	24
Informal Education (CompTIA Tec	---	3	5	4	6	6	3	medium/direct	4	0	24	12	20	16	24	24	12
Informal Education (CISCO Tech C	---	3	3	4	4	3	3	medium/direct	4	0	24	12	12	16	16	12	12
Informal Education (Trade Schools	---	6	6	6	6	6	6	high/direct	6	0	36	36	36	36	36	36	36
Informal Education (Youtube Top F	2017	5	3	1	6	2	4	medium/direct	4	0	24	20	12	4	24	8	16
Malware in National Language	---	3	6	3	6	6	3	medium/direct	4	0	24	12	24	12	24	24	12
Conduct																	
CERT Conduct	---	3	6	2	1	5	4	medium/indirect	3	0	18	9	18	6	3	15	12
Culture	---	6	5	2	5	3	0	high/indirect	5	0	30	30	25	10	25	15	0
Cyber Policy	---	5	6	5	6	5	0	medium/indirect	3	0	18	15	18	15	18	15	0
Cybersecurity Council	---	0	6	6	6	0	0	low/indirect	1	0	6	0	6	6	6	0	0
Declared Cyber Command	---	6	6	1	6	0	0	low/indirect	1	0	6	6	6	1	6	0	0
Freedom House Rating	2017	1	4	2	3	5	6	low/indirect	1	0	6	1	4	2	3	5	6
Hacking Team Software	---	0	6	0	6	6	6	medium/indirect	3	0	18	0	18	0	18	18	18
Norms	---	4	4	4	2	4	2	high/indirect	5	0	30	20	20	20	10	20	10
Offensive/Defensive	---	4	4	4	4	6	4	high/indirect	5	0	30	20	20	20	20	30	20
Strong Focus on Military	---	6	6	0	6	6	6	high/direct	6	0	36	36	36	0	36	36	36
CAPABILITY SUB-TOTAL										0	810	570	629	466	641	521	451
CAPABILITY SUB-TOTAL RATIO										0	1	0.704	0.777	0.575	0.791	0.643	0.557
Motivation																	
APT Groups	---	0	6	6	0	6	6	high/indirect	5	0	30	0	30	30	0	30	30
Blocked Access	---	6	6	6	6	6	6	medium/indirect	3	0	18	18	18	18	18	18	18
Curiousity	---	5	5	5	4	1	0	medium/direct	4	0	24	20	20	20	16	4	0
Domestic Politics	---	3	3	5	4	5	4	high/direct	6	0	36	18	18	30	24	30	24
Geopolitics	---	4	4	6	2	4	5	high/direct	6	0	36	24	24	36	12	24	30
Inequality in Income (SWIID Rank)	---	6	3	5	4	1	2	high/direct	6	0	36	36	18	30	24	6	12
Patriotism/Hacktivism	---	6	6	6	4	6	3	high/direct	6	0	36	36	36	36	24	36	18
Previous Attacks	---	4	5	6	5	6	4	high/indirect	5	0	30	20	25	30	25	30	20
Pride/Ego	---	4	5	4	5	3	4	high/indirect	5	0	30	20	25	20	25	15	20
Religion	---	6	6	6	0	0	0	medium/direct	4	0	24	24	24	24	0	0	0
Screen Time (Number of Hours/Da	2014	5	5	5	6	5	6	low/indirect	1	0	6	5	5	5	6	5	6
Spying	---	4	4	6	2	4	5	high/direct	6	0	36	24	24	36	12	24	30
Unemployment Rate (% of Labor F	2015	5	2	6	4	1	3	high/direct	6	0	36	30	12	36	24	6	18
Website Defacements	2013	5	3	2	1	6	4	high/indirect	5	0	30	25	15	10	5	30	20
Youth Unemployment Rate (% of L	2015	6	4	5	3	1	2	high/direct	6	0	36	36	24	30	18	6	12
MOTIVATION SUB-TOTAL										0	444	336	318	391	233	264	258
MOTIVATION SUB-TOTAL RATIO										0	1	0.757	0.716	0.881	0.525	0.595	0.581
Opportunity																	
Budapest Convention (Signed/Rati	---	6	5	6	6	6	6	low/indirect	1	0	6	6	5	6	6	6	6
Cyber Crime Arrests/Indictments	---	3	4	6	2	1	4	high/direct	6	0	36	18	24	36	12	6	24
Cyber Enforcement	---	3	1	5	1	1	5	high/direct	6	0	36	18	6	30	6	6	30
Cyber Law	---	4	1	4	2	2	3	medium/indirect	3	0	18	12	3	12	6	6	9
Informal Economy (Black Market)	---	6	4	6	1	3	2	high/direct	6	0	36	36	24	36	6	18	12
Non-Align Movement (Member)	---	6	6	6	6	6	6	low/indirect	1	0	6	6	6	6	6	6	6
UN Group of Experts (Member)	---	6	5	6	6	6	6	low/indirect	1	0	6	6	5	6	6	6	6

Indicator	Year	Indonesia	Malaysia	Phillipines	Singapore	Thailand	Vietnam	Total Weight	Total Weight #	Minumum	Maximum	Indonesia Total	Malaysia Total	Phillipines Tota	Singapore Total	Thailand Total	Vietnam Total
OPPORTUNITY SUB-TOTAL										0	144	102	73	132	48	54	93
OPPORTUNITY SUB-TOTAL RATIO										0	1	0.708	0.507	0.917	0.333	0.375	0.646
Gender																	
Gender Development Index	2014	6	5	3	4	2	1	low/indirect	1	0	6	6	5	3	4	2	1
Gender Inequality Index	2015	5	1	4	6	2	3	medium/direct	4	0	24	20	4	16	24	8	12
Population with at least some seco	2015	2	5	3	6	1	4	medium/indirect	3	0	18	6	15	9	18	3	12
Population with at least some seco	2015	2	5	4	6	1	3	medium/indirect	3	0	18	6	15	12	18	3	9
GENDER SUB-TOTAL										0	66	38	39	40	64	16	34
GENDER SUB-TOTAL RATIO										0	1	0.576	0.591	0.606	0.970	0.242	0.515
Investment																	
Investment	---	5	6	6	6	4	4	high/direct	6	0	36	30	36	36	36	24	24
INVESTMENT SUB-TOTAL										0	36	30	36	36	36	24	24
INVESTMENT SUB-TOTAL RATIO										0	1	0.833	1.00	1.000	1.00	0.667	0.667
CYBER THREAT ACTIVITY SCORE:										0	1500	1076	1095	1065	1022	879	860
CYBER THREAT ACTIVITY SCORE RATIO:										0	1	0.717	0.730	0.710	0.681	0.586	0.573

12. Works Cited

"About Us." Cyber Scout Thailand. Last modified 2017. http://www.cyberscout.in.th/about.php.

"About CoderSchool." CoderSchool. http://www.coderschool.vn/about

"Access to electricity (% of population)." The World Bank. http://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=ID-MY-PH-SG-TH-VN.

Aiken, Klée, and Jessica Woodall. *Asia-Pacific Cyber Insights*. Barton, Australia: Australian Strategic Policy Institute, 2015. https://www.aspi.org.au/publications/asia-pacific-cyber-insights.

Aiken, Klee. Interview by the author. February 16, 2017.

Angelidou, Margarita. "Smart City Strategy: Cyberjaya (Malaysia)." Urenio. http://www.urenio.org/2015/02/09/smart-city-strategy-cyberjaya-malaysia/.

APT30 and the Mechanics of a Long-running Cyber Espionage Operation. FireEye iSIGHT, n.d. https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

"APT Groups and Operations." Working paper, n.d. https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/htmlview.

Ashford, Warwick. "Thai military to recruit civilian "cyber warriors"." Computer Weekly. Last modified January 4, 2017. http://www.computerweekly.com/news/450410360/Thai-military-to-recruit-civilian-cyber-warriors.

"Bachelors, masters constitute 20% of unemployed people in Vietnam." Tuoi Tre News. Last modified December 27, 2015. http://tuoitrenews.vn/society/32459/bachelors-masters-constitute-20-of-unemployed-people-in-vietnam.

Bannier, Betsy J. "Global Trends in Transnational Education," International Journal of Information and Education Technology." 6:1, January 2016.

Banyan. "Hacking in Singapore Messiah complicated." The Economist. Last modified December 7, 2013. http://www.economist.com/blogs/banyan/2013/12/hacking-singapore.

Barrett, Devlin. "U.S. Charges Man in Malaysia With Hacking Aiding Islamic State." The Wall Street Journal. Oct. 15 2015. https://www.wsj.com/articles/u-s-charges-man-in-malaysia-with-hacking-aiding-islamic-state-1444950858

Blum-Dumontet, Eva. "Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand." Privacy International. Last modified September 20, 2016. https://www.privacyinternational.org/node/935.

"Browse Schools." Course Report. https://www.coursereport.com/.

Central Intelligence Agency. "Indonesia." The World Factbook. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/id.html.

———. "Malaysia." The World Factbook. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/my.html.

———. "The Philippines." The World Factbook. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/rp.html.

———. "Singapore." The World Factbook. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/sn.html.

———. "Thailand." The World Factbook. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/th.html.

———. "Vietnam." The World Factbook. Last modified 2017. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/vm.html.

CIA. "Internet Service Providers (ISPs) - The World Factbook - CIA." World Fact Book. http://www.nationsencyclopedia.com/WorldStats/CIA-Internet-Service-Providers-ISPs.html.

"CISA, CISM, CGEIT and CRISC Certifications." ISACA. Last modified 2017. http://www.isaca.org/Indonesia/Certification/Pages/Default.aspx.

The Citizen Lab Southeast Asia Cyberwatch: June 2013. Munk School of Global Affairs, 2013. https://citizenlab.org/publications/.

Chalmers, John, and Karen Lema. "For bank heist hackers, the Philippines was a handy black hole." Reuters. March 21, 2016. Accessed April 19, 2017. http://www.reuters.com/article/us-usa-fed-bangladesh-philippines-idUSKCN0WM13B.

Chinese Firm Outs "OceanLotus Group: A Nexus with Vietnam? FireEye iSIGHT Intelligence. April 29 2016. Print.

Clark, Nick, ed. "Education in Malaysia." World Education News & Reviews. Last modified December 2, 2014. http://wenr.wes.org/2014/12/education-in-malaysia.

———, ed. "Education in Thailand." World Education News & Reviews. Last modified March 3, 2014. http://wenr.wes.org/2014/03/education-in-thailand.

"CompTIA A+." CompTIA. Last modified 2017. https://certification.comptia.org/certifications/a.

"CompTIA A+ Classes in Jakarta, Indonesia." CompTIA. https://www.netcomlearning.com/training/comptia-a+/jakarta-indonesia.html.

"CompTIA A+ Classes in Manila, Philippines." NetCom Learning. Last modified 2017. https://www.netcomlearning.com/training/comptia-a+/manila-philippines.html.

"CompTIA Thailand." CompTIA. https://www.comptia.org/international/thailand/home.

CompTIA Thailand." CompTIA Information Technology. October 2012. https://www.comptia.org/international/thailand/home.

"CompTIA Training at New Horizons Singapore." New Horizons. http://newhorizons.com.sg/comptia/.

“Country: Vietnam.” The Software Alliance. Asia-Pacific Cybersecurity Dashboard. 2015. Web. http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_vietnam.pdf

“Cybercrime Investigation and Coordinating Center (CICC) | DICT” Republic of the Philippines. Web. http://www.dict.gov.ph/cybercrime-investigation-and-coordinating-center-cicc/

Cyber Law Asia, “Cyber Laws in Asia,” 2010. Web. http://cyberlawasia.com/cyber-laws-asia/

Cyber Maturity in the Asian-Pacific Region 2016. Barton, Australia: International Cyber Policy Centre, 2016. https://www.aspi.org.au/publications/cyber-maturity-2016/ASPI-Cyber-Maturity-2016.pdf.

Cyber Security Capability Maturity Model - CMM - Pilot. Oxford, U.K.: University of Oxford - Global Cyber Security Capacity Center, 2014. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front.

Cyber Threat Insider Blog, “#OpSaveGaza Campaign – Insights from the Recent Anti-Israel Cyber Operation,” August 11, 2014. Web. https://blog.sensecy.com/tag/icr/

"Cyberwellness Profile Thailand." Information Telecommunications Union. Last modified December 17, 2014. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Thailand.pdf.

de Hann, Jarryd. "Malaysia: Many Challenges to Wawasan 2020 Development Vision." Future Directions International. Last modified June 14, 2016. http://www.futuredirections.org.au/publication/malaysia-many-challenges-wawasan-2020-development-vision/.

Del Puerto, Jake. "Introduction: Philippine Cybercrime Law." Cybercrime Law. Last modified October 16, 2015. http://cybercrimelaw.ph/42/introduction-philippine-cybercrime-law/.

Department of Statistics Malaysia, Press Release: Informal Sector Work Force Survey Report, Malaysia 2015, (DoS Malaysia: 2016). Web.https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=UUFsUEJnNGFhcDE1TndNUlg4OEZCQT09

"Details of Treaty No.185 Convention on Cybercrime." Council of Europe. Last modified 2017. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

Dikemanskini, Terakhir. “Malaysia and Philippines established cooperation on cyber security,” Agenda Daily. Dec 13 2016. Web. http://www.agendadaily.com/Business/malaysia-and-philippines-established-cooperation-on-cyber-security.html

"Education in Vietnam: Very good on paper." The Economist. Last modified December 12, 2013. http://www.economist.com/blogs/banyan/2013/12/education-vietnam.

"8 CCNA training centers in the Philippines." CCNA Philippines. Last modified February 9, 2017. https://www.ccnaphilippines.com/8-ccna-training-centers-in-the-philippines/.

“Education in Thailand,” World Education Services. March 3 2014. Web. http://wenr.wes.org/2014/03/education-in-thailand

"Employees by Sex and Occupation." In *ILOSTAT*. 2016. https://www.ilo.org

"FireEye Horizons: An Overview of How Nations Decide Whether to Build or Buy Their Offensive Cyber Capabilities." Unpublished manuscript, August 22, 2016.

"FireEye iSIGHT Intelligence Horizons – Fractured Cyberspace: A Risk Outlook for Multinational Businesses." Unpublished manuscript, June 22, 2016.

"Fixed broadband subscriptions (per 100 people)." The World Bank. http://data.worldbank.org/indicator/IT.NET.BBND.P2?locations=ID-MY-SG-PH-VN-TH.

Francisco, Katerina. "Online libel tops cybercrime cases in the Philippines for 2016." Rappler. Last modified January 27, 2017. http://www.rappler.com/newsbreak/iq/159365-cybercrime-philippines-cases-online-libel-2016.

"Freedom in the World: Anxious Dictators, Wavering Democracies: Global Freedom under Pressure." Raw data, 2016. https://freedomhouse.org/report/freedom-world/freedom-world-2016.

Gady, Franz-Stefan. Interview by the author. March 2, 2017.

Gannes, Liz. “Singapore Rising: The Plot to Be The Next Big Tech Hub”, Jun 16, 2015. Web. https://www.recode.net/2015/6/16/11563586/singapore-rising-the-plot-to-be-the-next-big-tech-hub

Gavilan, Jodesz. “The state of cybersecurity in the Philippines,” 2016. Web. http://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines

"Gender Inequality Index (GII)." In *Human Development Reports*. 2016. Last modified 2016. http://hdr.undp.org/en/content/gender-inequality-index-gii.

Giovanini, Gabriele & Emanuele Schibotto, “Singapore and the Asian Century”, February 19 2015, http://thediplomat.com/2015/02/singapore-and-the-asian-century/

Goh, Gabey. "Cybercrime: Malaysia not lagging but needs to level up." Digital News Asia. Last modified September 24, 2014. https://www.digitalnewsasia.com/security/cybercrime-malaysia-not-lagging-but-needs-to-level-up.

Graduate Employability in Asia. Bangkok, Thailand: UNESCO Bangkok, 2012. http://unesdoc.unesco.org/images/0021/002157/215706E.pdf.

Graham, Ian. "Unemployment Rate: Countries Compared." In *Nation Master*. http://www.nationmaster.com/country-info/stats/Labor/Unemployment-rate.

Gray, Michael L. "The Trouble with Vietnam's Cyber Security Law." The Diplomat. Last modified October 21, 2016. http://thediplomat.com/2016/10/the-trouble-with-vietnams-cyber-security-law/.

"G.R. No.204637." In *Republic of the Philippines Supreme Court G.R. No. 204637*. Republic of the Philippines Supreme Court, 2013. Last modified April 16, 2013. http://sc.judiciary.gov.ph/jurisprudence/2013/april2013/204637.pdf.

Han, Kirsten. "Singapore Cracks the Whip on Cyber 'Terrorism'." The Diplomat. Last modified November 29, 2013. http://thediplomat.com/2013/11/singapore-cracks-the-whip-on-cyber-terrorism/.

Haziq Bin Jani, Muhammad. "Urgent need to counter Malaysia's 'Cyber-ISIS.'" The Strait Times. Last modified March 29, 2016. http://www.straitstimes.com/asia/se-asia/urgent-need-to-counter-malaysias-cyber-isis.

Healey, Jason. Interview by the author. January 27, 2017.

Hein, Quy. "Vietnam jobless graduate numbers double in 4 years." Thanh Nien News. Last modified 2015. http://www.thanhniennews.com/education-youth/vietnam-jobless-graduate-numbers-double-in-4-years-42632.html.

Heller, Nathan. "Amos Yee: YouTube Star, Teen-ager, Dissident." The New Yorker. Last modified April 10, 2015. http://www.newyorker.com/culture/cultural-comment/the-arrest-of-a-teen-aged-youtube-star.

"India invites Vietnam to set up electronics cluster city." Business Line. http://www.thehindubusinessline.com/info-tech/india-invites-vietnam-to-set-up-electronics-cluster-city/article4881622.ece.

"Indonesia Computer Emergency Response Team." ID-CERT. https://www.cert.or.id/beranda/en/.

"Indonesian hackers launch Independence Day attack on Malaysian Websites," Networksasia, http://www.networksasia.net/article/indonesian-hackers-launch-independence-day-attack-malaysian-websites-1251878483

"Indonesian man arrested for hacking into an electronic billboard." SG Cyber Security. http://www.sgcybersecurity.com/indonesian-man-arrested-for-hacking-into-an-electronic-billboard/.

"Indonesian police arrest 31 Chinese suspected of cyber fraud." Vietnam Plus. Last modified June 22, 2016. http://en.vietnamplus.vn/indonesian-police-arrest-31-chinese-suspected-of-cyber-fraud/95063.vnp.

"Indonesian Student Detained Under Cyber Law for Police Extortion Video." GlobalVoices ADVOX. Last modified October 2, 2015. https://advox.globalvoices.org/2015/10/02/indonesian-student-detained-under-cyber-law-for-police-extortion-video/.

"Informal Economy." In *ILOSTAT*. 2016. https://www.ilo.org/

Ingram, Graham. "Asia Pacific Computer Emergency Response Team APCERT," Web. https://pdfs.semanticscholar.org/96d1/b28092c394ce158fff058b8420852ed8f888.pdf

"International drill on cyber security held in Vietnam," VietNamNet. March 3 2017. Web. http://english.vietnamnet.vn/fms/science-it/175099/international-drill-on-cyber-security-held-in-vietnam.html

"ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges." United States Department of Justice. Last modified October 15, 2015. https://www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges.

"Jakarta Globe." Jakarta Globe. Last modified 2017. http://jakartaglobe.id/news/indonesia-extradites-64-taiwanese-arrested-cyber-crime/.

Jusoh, Sufian, ed. "Cyber Related Policies and Laws in Malaysia." Cybersecurity Capacity Portal. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-related-policies-and-laws-malaysia.

"K-Team" YouTube Channel. 2017. https://www.youtube.com/channel/UCBw4b26KZrBvHRPBjOCw6UQ/videos

Kaw, Kamlang. "Sasiwimol: Mother's Day Without Mother." iLaw Freedom. Last modified September 21, 2015. https://freedom.ilaw.or.th/en/blog/sasiwimol-mother%E2%80%99s-day-without-mother.

Khoon, Goh Soo, Michael Lim Mah-Hui, "The Impact of the Global Financial Crisis: The Case of Malaysia. Third World Network. 2010. http://www.thirdworldnetwork.net/finance/file_dir/12190611054dd0cf08a5bf8.pdf

Kleiner, Aaron, Paul Nicholas, and Kevin Sullivan. *Linking Cybersecurity Policy and Performance*. Microsoft, 2013. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/microsoft-linking-cybersecurity-policy-and-performance.

Koswanage, Niluksi. "Malaysia tries to stop threatened Cyber Attack", Jun 15 2011, http://www.reuters.com/article/us-cyber-malaysia-idUSTRE75E05N20110615

Kovacs, Eduard. "Microsoft Office Flaw Exploited by Several APT Actors." Security Week. Last modified May 25, 2016. http://www.securityweek.com/microsoft-office-flaw-exploited-several-apt-actors.

———. "'Platinum' Cyberspies Abuse Hotpatching in Asia Attacks." Security Week. Last modified April 27, 2016. http://www.securityweek.com/platinum-cyberspies-abuse-hotpatching-asia-attacks.

Kundu, Nivedita Das. "NON ALIGNMENT MOVEMENT AND ITS SIGNIFICANCE." Valdai.

http://my.noodletools.com/web/bibliography.html.

Lamb, Kate. "'Anonymous Indonesia' Launches Cyber Attack on Government Sites." VOA. Last modified January 31, 2013. http://www.voanews.com/a/anonymous-indonesia-launches-cyber-attack-on-government-sites/1594318.html.

Leyden, John. "Malaysia-based credit card fraud ring broken, 105 arrested." The Register. Last modified July 8, 2016. https://www.theregister.co.uk/2016/07/08/credit_card_fraud_ring_busted/.

Lexology, "Data Security and Cybercrime in Vietnam," Global, Vietnam. 8, February 2017. Web. http://www.lexology.com/library/detail.aspx?g=37d6b3a7-f0aa-4a3f-8688-2e31967b1708

Lipton, Eric.,Sanger, David.,Shane, Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S., New York Times. December 13, 2016. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

Macapagal, Maan."WATCH: Men who pretend to be women nabbed in cybersex den raid" ABS-CBN News. July 28 2016. Web. http://news.abs-cbn.com/news/07/27/16/watch-men-who-pretend-to-be-women-nabbed-in-cybersex-den-raid

"Malaysia arrests five Filipinos for suspected Islamic State links." Reuters. http://news.trust.org/item/20170313054650-7jinr.

"MALAYSIA: END UNPRECEDENTED CRACKDOWN ON HUNDREDS OF CRITICS." Amnesty International. Last modified March 11, 2016. https://www.amnesty.org/en/press-releases/2016/03/malaysia-end-unprecedented-crackdown-on-hundreds-of-critics-through-sedition-act/.

"Malaysian citizens arrested for alleged role in cyber crime." The Jakarta Post. Last modified March 3, 2014. http://www.thejakartapost.com/news/2014/03/03/malaysian-citizens-arrested-alleged-role-cyber-crime.html.

"Mapping Hacking Team's "Untraceable" Spyware." Citizen Lab. February 17 2014. Web. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

"Many wonder about the extent of cyber army's jurisdiction." The Nation. October 26, 2015. http://www.nationmultimedia.com/news/national/aec/30271668.

Mongkolnchaiarunya, Jittip. Interview by the author. February 16, 2017.

———. "The Trouble With Thailand's New Cyber Approach." The Diplomat. Last modified August 4, 2016. http://thediplomat.com/2016/08/the-trouble-with-thailands-new-cyber-approach/.

"MY-CERT." MY-CERT. https://www.mycert.org.my/en/.

Nash, Charlie. "'Offensive' Memes Can Lead to Jail Time Under Indonesia 'Cyberbullying' Laws." Breitbart. Last modified October 5, 2016. http://www.breitbart.com/tech/2016/10/05/offensive-memes-can-lead-to-jail-time-under-indonesia-cyberbullying-laws/.

Nathan, David. "Thailand's youth asked to cyber-spy for the state." New Internationalist. https://newint.org/features/web-exclusive/2014/09/05/thailand-cyber-crackdown/.

Ngui, Yantoultra, and Mark Hosenball. "Malaysia arrests hacker for supplying U.S. targets to Islamic State." Reuters. Last modified October 15, 2015. http://www.reuters.com/article/us-malaysia-islamic-state-idUSKCN0SA05R20151016.

"Nine Hackers Arrested in Thailand Over Government Hacking." Newsweek. Last modified December 26, 2016. http://www.newsweek.com/nine-hackers-arrested-thailand-over-government-hacking-536315.

"The Non-Aligned Movement." The Non-Aligned Movement. Last modified 2017. http://www.nam.gov.za/media/040802b.htm.

Nugroho, Wibawanto. "Indonesia and the globalization of religious terrorism," September 09, 2016. Web. http://www.thejakartapost.com/academia/2016/09/09/ri-and-the-globalization-of-religious-terrorism.html

"Obama highlights ASU during trip to Vietnam." ASU Now. May 26 2016. Web. https://asunow.asu.edu/20160523-global-engagement-obama-mentions-asu-during-trip-vietnam

OECD, Structural Policy Country Notes Malaysa, (OECD: 2012), p. 4-7 Web. https://www.oecd.org/dev/asia-pacific/Malaysia.pdf

"OIC-CERT." OIC-CERT. Last modified 2017. https://www.oic-cert.org/en/.

OIC-CERT, "Cybersecurity Malaysia Appointed As Secretariat to OIC-CERT," 2013. Web. https://www.oic-cert.org/en/newsletter.html

"Opportunities." Privacy International. Last modified 2017. https://privacyinternational.org/node/78.

Orendain, Simone. "Philippines Files Pleadings in Case Against China," VOA March 30 2014. Web. http://www.voanews.com/a/philippines-files-pleadings-in-case-against-china/1882322.html

Othman, Lilyana. "Singapore's crime up 4% in 2015, driven by cybercrime." Channel NewsAsia. http://www.channelnewsasia.com/news/singapore/singapore-s-crime-up-4-in-2015-driven-by-cybercrime-8177276.

Palatino, Mong. "The Truth About Thailand's Social Media Surveillance." The Diplomat. Last modified October 3, 2016. http://thediplomat.com/2016/10/the-truth-about-thailands-social-media-surveillance/.

Pham, Hiep. "Graduate unemployment and 'over-education' rising." University World News. http://www.universityworldnews.com/article.php?story=20130711163808113.

Poh, Ian. "Singapore Cyber Attacks: Suspected hackers and vandals arrested." If Only Singaporeans Stopped to Think. Last modified January 30, 2015.

http://ifonlysingaporeans.blogspot.com/2013/11/suspected-hackers-and-vandals-arrested.html.

"Population and Labor Force (Sex, Age and Education)." ILOSTAT. Last modified 2016. https://www.ilo.org

"Population with at Least Secondary Education, Female/male Ratio (Ratio of Female to Male Rates)." In *Human Development Reports*. 2016. Last modified 2016. http://hdr.undp.org/en/content/population-least-secondary-education-femalemale-ratio-ratio-female-male-rates.

"Privacy International." Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand. September 20, 2016. Accessed April 19, 2017. https://www.privacyinternational.org/node/935.

Rahwidiati, Diastika, and George Hodge. "Imagining a Data Empowered Village." United Nations Global Pulse: Harnessing big data for development and humanitarian action. http://unglobalpulse.org/imagining-data-empowered-village.

Republic of the Philippines. "Department of Information Communications Technology." Cybersecurity | DICT. http://www.dict.gov.ph/cybersecurity/.

"Research shows university graduates still have highest unemployment rate." Thai PBS. Last modified February 29, 2016.

Reuters. "MALAYSIA ARRESTS 7 FOR SUSPECTED LINKS TO TERROR GROUPS INCLUDING ISIS." The Jerusalem Post. Last modified March 5, 2017. http://www.jpost.com/Breaking-News/Malaysia-arrests-7-for-suspected-links-to-terror-groups-including-ISIS-483260.

The Right to Privacy in Thailand. Stakeholder Report no. 25. September 2015. https://privacyinternational.org/sites/default/files/privacy_thailand.pdf.

Roady, Peter. Interview by the author. February 8, 2017.

Ruiz, Neil G. *The Geography of Foreign Students in U.S. Higher Education: Origins and Destinations*. Washington, DC: Brookings Institute, 2014. https://www.brookings.edu/interactives/the-geography-of-foreign-students-in-u-s-higher-education-origins-and-destinations/.

"Running Afoul of the Thai Monarchy." The New York Times. April 19, 2017. https://www.nytimes.com/interactive/2015/09/18/world/asia/thailand-king-lese-majeste.html.

Saiyasombut, Saksith. "Thailand Junta Reactivates 'Cyber Scout' Program to Curb Online Dissent." Asian Correspondent. Last modified August 7, 2014. https://asiancorrespondent.com/2014/08/thailand-junta-reactivates-cyber-scout-program-to-curb-online-dissent/#GZcWWxwh7rBp5WK1.97.

Sasivimol: *Posted messages on Facebook*. 2017. https://freedom.ilaw.or.th/en/case/681#progress_of_case.

"Secondary Education in Vietnam." World Education News & Reviews. Last modified April 2, 2012. http://wenr.wes.org/2012/04/secondary-education-in-vietnam.

"Secure Internet servers." The World Bank. http://data.worldbank.org/indicator/IT.NET.SECR?locations=ID-MY-SG-PH-VN-TH.

Segal, Adam. "The UN's Group of Governmental Experts on Cybersecurity." Council on Foreign Relations. Last modified April 13, 2015. http://blogs.cfr.org/cyber/2015/04/13/the-uns-group-of-governmental-experts-on-cybersecurity/.

Sibunruang, Atchaka. "Thailand Moving Ahead with Cluster Development." Infographic. Ministry of Industry. November 23, 2015.http://www.boi.go.th/upload/content/Presentation%20by%20Minister%20of%20Industry_89274.pdf.

Silencing the Messenger: Communication Apps Under Pressure. Freedom House, 2016. https://freedomhouse.org/report/freedom-net/freedom-net-2016.

"Singapore," Forbes. 2017. Web. https://www.forbes.com/places/singapore/

"Singapore Cybersecurity Consortium." Singapore Cybersecurity Consortium. http://sgcsc.sg/.

"Singapore's Cybersecurity Strategy." CSA Singapore. Last modified October 10, 2016. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy.

"SingCERT." SingCERT. https://www.csa.gov.sg/singcert.

The Software Alliance. "Country: Indonesia." Asia Pacific Cybersecurity Dashboard. http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_indonesia.pdf.

Stern, Matthew. "Malaysian Government Initiative Built on CompTIA A+." CompTIA. Last modified September 29, 2016. https://certification.comptia.org/it-career-news/post/view/2016/09/29/malaysian-government-initiative-built-on-comptia-a.

"Taiwanese Nationals Arrested On Suspicion Of Cyber Crime Charges." Indonesia Expat. Last modified April 13, 2013. http://indonesiaexpat.biz/topreads/taiwanese-nationals-arrested-on-suspicion-of-cyber-crime-charges/.

"Tech4ED Platform | eSociety - Information and Communications Technology Office." Republic of the Philippines. http://dict.gov.ph/tech4ed/tech4ed/tech4ed-platform/

"ThaiCERT." ThaiCERT. https://www.thaicert.or.th/about-en.html.

"Thai demand for higher education cooling as population ages." ICEF Monitor. Last modified July 12, 2016. http://monitor.icef.com/2016/07/thai-demand-higher-education-cooling-population-ages/.

"Thailand: Digital Ministry Established as Part of National Digital Economy Plan." Global Legal Monitor. http://www.loc.gov/law/foreign-news/article/thailand-digital-ministry-established-as-part-of-national-digital-

economy-plan/.

"Thailand faces big risk from malware." The Nation. October 28, 2015. Accessed April 19, 2017. http://www.nationmultimedia.com/news/national/aec/30271838.; "RIPPER ATM Malware Linked to Thailand Heist." Information Security News, IT Security News & Expert Insights: SecurityWeek.Com. Accessed April 19, 2017. http://www.securityweek.com/ripper-atm-malware-linked-thailand-heist.

Thai IT Students Gain Competitive Edge with CompTIA Certifications. December 1, 2016. Accessed April 19, 2017. https://certification.comptia.org/it-career-news/post/view/2016/12/01/thai-it-students-gain-competitive-edge.

"Thai police arrest Russian, Uzbeki for alleged cybertheft." Phys. Last modified July 21, 2016. https://phys.org/news/2016-07-thai-police-russian-uzbeki-alleged.html.

"Thai police create fake FB app to get Thai net users' information, target users trying to open blocked sites." Prachatai English. Last modified June 20, 2014. https://prachatai.com/english/node/4140.

"3 PH universities included in int'l employability list." ABS CBN. Last modified November 25, 2016. http://news.abs-cbn.com/life/11/24/16/3-ph-universities-included-in-intl-employability-list.

"Total Unemployment Rate (% of Labour Force)." In *United Nations Development Programme Human Development Reports*. http://hdr.undp.org/en/indicators/140606.

"Trends in Graduate Employability: Key Findings From The MEM Report." Talent Corp Malaysia. Last modified 2015. https://www.talentcorp.com.my/facts-and-figures/matching-talents-to-jobs.

"Two for One: Microsoft Office Encapsulated PostScript and Windows Privilege Escalation Zero-Days." Unpublished manuscript, n.d. https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf.

"2016 Human Development Report: Gender Development Index." In *Human Development Report*. 2016. Accessed 2017. http://hdr.undp.org/en/2016-report.

UltimaRatioReg. "Indictment of Malaysian Cyber Criminal Arrested at JFK." U.S. Naval Institute. Last modified November 2010. https://blog.usni.org/2010/11/22/indictment-of-malaysian-cyber-criminal-arrested-at-jfk.

"UNCT, Thailand Submission." Universal Periodic Review. May 25, 2016. https://www.upr-info.org/sites/default/files/document/thailand/session_25_-_may_2016/rco_upr25_tha_e_main.pdf.

Universal Periodic Review (UPR) UNCT, Thailand Submission. https://www.upr-info.org/sites/default/files/document/thailand/session_25_-_may_2016/rco_upr25_tha_e_main.pdf.

(UPDATE) Filipino hackers fight back, deface Chinese sites, INQUIRER.net, http://technology.inquirer.net/10235/filipino-hackers-fight-back-deface-chinese-sites

Urbas, Greg. *An Overview of Cybercrime Legislation and Cases in Singapore*. Singapore: Asia Law Institute, 2008. http://law.nus.edu.sg/asli/pdf/WPS001.pdf.

"Vietnam: Arrests of Internet Activists Escalate." Human Rights Watch. Last modified May 17, 2014. https://www.hrw.org/news/2014/05/07/vietnam-arrests-internet-activists-escalate.

"Vietnamese blogger arrested on anti-state charges." Committee to Protect Journalists. Last modified May 7, 2014. https://cpj.org/2014/05/vietnamese-blogger-arrested-on-anti-state-charges.php.

"Vietnam: Helping 8,000 Poor Students Pursue Their Academic Dreams." The World Bank. Last modified April 10, 2014. http://www.worldbank.org/en/results/2014/04/10/vietnam-helping-8000-poor-students-pursue-their-academic-dreams.

"Vietnam: New Round of Arrests Target Democracy Activists Prominent Blogger Sentenced to Prison." Human Rights Watch. Last modified September 12, 2008. https://www.hrw.org/legacy/english/docs/2008/09/11/vietna19796.htm.

"VN-CERT." VN-CERT. http://www.vncert.gov.vn/.

"Vnohow (Thailand) Co., Ltd." Cisco. http://www.cisco.com/c/th_th/training-events/training-center.html.

Wasem, Ruth Ellen. *Immigration of Foreign Nationals with Science, Engineering, Technology and Mathmatics (STEM) Degrees*. November 26, 2012. https://www.hsdl.org/?view&did=726883.

"World Bank Indicators: Internet users (per 100 people)." UNdata. http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3AIT.NET.USER.P2.

Yap, Karl Lester M, "Rising Tiger Philippines Posts some of the World's Fastest Growth," Bloomberg. https://www.bloomberg.com/news/articles/2017-01-26/asia-s-new-growth-leader-takes-over-from-fading-tiger-economies

Yen Yen, Ooh. "The Budapest Treaty: on its way to Malaysia?" World Intellectual Property Review. http://www.worldipreview.com/contributed-article/the-budapest-treaty-on-its-way-to-malaysia.

Zeldin, Wendy. *Vietnam: Crackdown on Cyber-Activists, Including Prominent Lawyer*. Washington D.C., 2009. http://www.loc.gov/law/foreign-news/article/vietnam-crackdown-on-cyber-activists-including-prominent-lawyer/.

About the Authors

Lyndon Low served as the Presentation Editor on this project. Lyndon is a student at Columbia University's School of International and Public Affairs earning an MIA with a concentration in International Finance and Economic Policy. Lyndon specializes in Management. Prior to SIPA, Lyndon worked for the Department of Homeland Security on a Port Security project. Lyndon has traveled extensively in SouthEast Asia and offered invaluable cultural expertise during the project.

Daniel Schnok served as the Project Manager and Client Liaison on this project. Daniel is a student at Columbia University's School of International and Public Affairs earning an MPA with a concentration in International Security Policy. Daniel specializes in Management. Prior to SIPA, Daniel worked as a Policy Officer in the Federal Ministry for Economic Affairs on digital market issues for German companies in East Asia. Daniel's management studies and previous experience, in addition to his regional expertise were immeasurable benefits during this project.

Mena Tajrishi served as the Editor on this project. Mena is a student at Columbia University's School of International and Public Affairs earning an MPA with a concentration in International Security Policy. Mena is specializing in the Gender & Public Policy and will be pursuing a PhD following SIPA in which, Mena will attempt to bridge the intersection of cyber spheres and queer theory. Previously, Mena worked as a researcher, writer and activist for labor and LGBTQ issues, which more than adequately prepared Mena to serve as the editor on this project.

Jamie Welch served as the Fieldwork and Data Coordinator as well as the SIPA Liaison on this project. Jamie is a student at Columbia University's School of International and Public Affairs earning an MPA with a concentration in International Security Policy, where she completes mostly cyber-related coursework. She specializes in Applied Science, where she focuses mainly on data and information technology coursework. Jamie has completed numerous research jobs and data projects that prepared her to serve as the data coordinator.

Katheryn Rosen served as the Faculty Advisor on this project. Katheryn is an Adjunct Professor at Columbia University's School of International Public Affairs focusing on cybersecurity and a non-Resident Senior Fellow at the Atlantic Council – Brent Scowcroft Center on International Security's Cyber Statecraft Initiative. Over a 25-year career, Katheryn has been active in both the public and private sectors. She served at the U.S. Department of Treasury as Deputy Assistant Secretary for Financial Institutions Policy and Senior Advisor to the Assistant Secretary of Financial Institutions. On Capitol Hill, she served as Senior Policy Advisor to House Financial Services Chairman Barney Frank, working primarily on the Dodd-Frank Act and housing finance reform. In the private sector, Katheryn, a Managing Director at both JPMorgan and BlackRock, led teams and advised and executed transactions for a wide range of clients including GSEs, multilateral-lending institutions, government corporations, financial institutions and others on matters of financial regulation, fundraising, capital, liability restructuring, and risk management.

This report was produced for FireEye iSIGHT as part of a 2017 Capstone Project for Columbia University's School of International Public Affairs.