Bridging the Cyber Gap: Bilateral Cyber Relationships in the South China Sea

Word Count: 3499

A paper submitted to the Faculty of the United States Naval War College, Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations.

DISTRIBUTION A. Approved for public release: distribution unlimited.

The contents of this paper reflect the author's own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 26-04-2021	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)* N/A

4. TITLE AND SUBTITLE

Bridging the Cyber Gap: Bilateral Cyber Relationships in the South China Sea

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Rebecca F. Russo, Lt Col, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

In the last decade, China has increased its asymmetric approach to dealing with territorial disputes in the South China Sea, especially within the cyber domain. The United States is rightly concerned about China's increased cyber-attacks against Association of Southeast Asian Nations (ASEAN) with whom China harbors territorial disputes. The United States must develop effective bilateral cybersecurity coordination with three of the most influential nations in the region to counter China's provocative actions or risk further deterioration of United States influence. First, China is aggressively increasing its attacks against competing nations in the South China Sea. Second, ASEAN has limitations as a regional cyber leader, rendering them ineffective in this domain on a timeline of relevance. Third, the United States must invest in bilateral cyber relationships with Singapore, Vietnam, and the Philippines to counter China's malign activities in the South China Sea and protect United States' interests in the region. Therefore, to secure the global commons and ensure freedom of navigation through cyber, the United States military should immediately invest in bilateral cyber relationships to ensure an increase in resiliency against Chinese tactics, to grow emerging relationships in cyber, and ultimately deter China from its continued predatory actions in the South China Sea.

15. SUBJECT TERMS (Key words)
Cyber, relationships, cyber maturity, South China Sea, China, Vietnam, Singapore, Philippines, cyber-attack, defensive, security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Director, Writing Center
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED	N/A		**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6499

The United States' strategic competitors are conducting cyber-enabled campaigns to erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity. The Department must respond to these activities by exposing, disrupting, and degrading cyber activity threatening U.S. interests, strengthening the cybersecurity and resilience of key potential targets, and working closely with other departments and agencies, as well as with our allies and partners.

~2018 Department of Defense Cyber Strategy

INTRODUCTION

In the last decade, China has increased its asymmetric approach to dealing with territorial disputes in the South China Sea, especially within the cyber domain. The United States is rightly concerned about China's increased cyber-attacks against Association of Southeast Asian Nations (ASEAN) with whom China harbors territorial disputes. These behaviors against regional nations will increase as China looks to counter any protest to its territorial claims and influence its version of international cyber norms. According to the RAND study, *The Thickening Web of Asian Security Cooperation*, "China's ultimate geopolitical objective is to push the United States out of the Asia-Pacific."[1] The United States however, is an interested and influential partner in this domain and must take additional aims to combat China's provocative cyber behavior, specifically using robust security cooperation within the military instrument of power. The United States must develop effective bilateral cybersecurity coordination with three of the most influential nations in the region to counter China's provocative actions or risk further deterioration of influence. First, China is aggressively increasing its attacks against competing nations in the South China Sea. Second, ASEAN has limitations as a regional cyber leader, rendering them ineffective in this domain on a timeline of relevance. Third, the United States must invest in bilateral cyber relationships with Singapore, Vietnam, and the Philippines to

[1] Scott W. Harold et al., *The Thickening Web of Asian Security Cooperation: Deepening Defense Ties Among U.S. Allies and Partners in the Indo-Pacific* (RAND Corporation, 2019), 278.

counter China's malign activities in the South China Sea and protect United States' interests in the region.

AN EMBOLDEND CHINA – INCREASING CYBER-ATTACKS

China's strategy, history of attributed offensive attacks, and study of historical precedent directly correlate to its increase in cyber-attacks on competing countries. First and foremost, cyber effects can be challenging to attribute to the initiator. Additionally, such effects have rarely resulted in armed conflict. Therefore, cyber conflict is a relatively easy way for an actor to use low-cost, highly available tools to create harmful effects across any instrument of power. China's overarching military strategy is to continually exploit the competition continuum below the level of armed conflict and uphold the "Chinese tradition of "subjugating the enemy without fighting.""[2] China's use of cyberspace effects has increased over time and is in direct support of its desire to "safeguard national sovereignty, unity, territorial integrity and security."[3] China also adopted a systems warfare approach whereby focusing on destroying or disrupting the opponent's operations systems, so they no longer have the ability to fight.[4] Similarly, China's cyber strategy demands "the use of information […] to influence or control the direction of an opponent's decision making activity."[5] Thus, cyber effects are an excellent asymmetric option for China to deter or retaliate against other countries' claims to territory in the South China Sea without fear of kinetic retaliation.

[2] Angela Poh and Weichong Ong, "PLA Reform, a New Normative Contest, and the Challenge for ASEAN," Asia policy 14, 14, no. 4 (2019): 112.

[3] Anthony H. Cordesman, "China's New 2019 Defense White Paper," Policy File (Center for Strategic and International Studies, 2019), 7.

[4] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018), ix-xiii.

[5] Miguel Alberto Gomez, "Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN," Journal of Communication and Computer 10, (2013): 799.

In addition to a strategy supporting China's use of cyber effects, multiple examples demonstrate its increase in frequency and severity of cyber-attacks to influence China's opponents. According to the Center for Strategic and International Studies, major attributable cyber-attacks from China have increased over 340 percent since 2007 with no hope of decreasing due to its systems-based warfare approach.[6] More specifically, in 2012, PRC sponsored hackers launched defacement and distributed denial of service (DDOS) attacks against the Philippines to retaliate against its territorial claims in the South China Sea.[7] In 2017, attributed Chinese cyber-attacks were launched against India, Indonesia, Vietnam, the Philippines, and Singapore, attacking high-level government representatives to steal passwords, access government systems, and gather intelligence on individuals' whereabouts.[8] As recent as April of this year, Chinese hackers targeted Vietnamese government officials with a punishing phishing campaign amid the on-going territorial dispute between the two nations.[9] This gives little doubt that China will continue to increase the volume and severity of cyber-attacks against nations with whom it harbors territorial disputes and any supporters. In addition to retaliatory type actions, there is historical precedence for cyber operations supporting forced land reclamation.

China is astutely aware of Russia's approach to Crimea's annexation and uses it as an exemplar in hybrid operations, blending cyber and traditional domains for land reclamation. In early 2014, Russia used extensive information operations and cyber-attacks to support its invasion and annexation of Crimea from Ukraine.[10] Through a combination of DDOS attacks,

[6] "Significant Cyber Incidents | Center for Strategic and International Studies."

[7] Gomez, "Awaken the Cyber Dragon: China's Cyber Strategy and Its Impact on ASEAN," 801. A distributed denial of service (DDOS) attack occurs when a website is flooded with so much traffic that it renders the website unusable.

[8] Jeevan Vasagar and Leo Lewis, "Chinese Hackers Shift Focus to Asia after US Accord," FT.com, 2017, n/a,

[9] Shannon Vavra, "Suspected Chinese Hackers Aim Attacks at Vietnamese Government Officials," CyberScoop, 2020, https://www.cyberscoop.com/south-china-sea-maritime-hacking-vietnam/.

[10] Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: Rand Corporation, 2017), 6–9.

disabling the electronic election system, and social media denial, Russia maintained a competitive advantage and hindered Ukraine's command and control that led to the physical repossession of Crimea.[11] The international community has done little to hold Russia accountable for this violently aggressive act. Thus, the precedence exists for cyber-attacks supporting territorial repossession with little international repercussion. Shortly after Russia's actions, China began building up features in the South China Sea and constructed military bases on newly developed islands to justify its claim to those territories.[12] This island building was likely because China knew the North American Treaty Organization (NATO) would not penalize them due to similar inaction after Russia's annexation of Crimea.[13] With China's strategy clearly outlining an increase in information operations to wield systems warfare, an increase in frequency and severity of cyber-attacks against Southeast Asian neighbors, and historical precedence for cyber-attacks supporting land reclamation without accountability, there must be a regional or global counterbalance to China's malign activities. ASEAN should be the regional leader, but has limitations in the newest human-made domain.

ASEAN LIMITATIONS AS A REGIONAL CYBER LEADER

One would assume that ASEAN is the prime regional organization to help members counter China's malign cyber activities with an increased focus on cybersecurity, intense desire for regional cyber norms, and the rapidly growing digital economy. However, due to the difficulty of reaching consensus, the nature of sovereign territories to focus on domestic policy over regional needs, and a difference in cyber maturity, ASEAN is hard-pressed to counter China's omnipresent threat in the cyber domain at the speed of relevance.[14] Southeast Asia is

[11] Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, 50–52.
[12] Walter C. Clemens, "Cyber and Other Powers in Asia," Asian perspective 43, 43, no. 3 (2019): 586.
[13] Walter C. Clemens, "Cyber and Other Powers in Asia," 586.
[14] Shashi Jayakumar, "Will there be One ASEAN Voice on Cyber?" Newstex..

one of the fastest-growing Internet economies globally, “hitting $100 billion in 2019, and 90% of the region's 360 million internet users connecting primarily through their mobile devices.”[15] This means that cybersecurity will continue to be vital to countries in the South China Sea since every digital connection constitutes an additional cyber-attack surface for the adversary. Since 2015, ASEAN has taken legitimate steps to increase its commitment to promoting cybersecurity and international norms while maintaining its heterogeneous cultural identity and commitment to consensus building.[16] By creating the 2017 ASEAN Cybersecurity Cooperation Strategy, the 2018 ASEAN Ministerial Conference on Cybersecurity, and the ASEAN Information and Communication Technologies (ICT) Masterplan 2020, one can see the strategic commitment to cybersecurity and the critical linkages amongst all members.[17] However, despite a deep commitment to these basic principles and norms, ASEAN struggles to reach consensus, which drives varied cybersecurity implementation.

ASEAN's strong culture grounded in sovereignty and consensus-building makes ASEAN less than ideal as the sole regional partner to counter China's cyber actions. The heterogeneous regional regimes, combined with the desire for consensus among all nations and particular sensitivity to any norms that could jeopardize sovereignty cause ASEAN to work at the slowest participant's pace.[18] Cyber norms are particularly susceptible to this cultural phenomenon since there are multiple approaches to how sovereignty applies in this human-made domain. Consequently, despite ASEAN's desire for advancement in cybersecurity policy, its habit of ruling via consensus at the slowest member's speed significantly limits its ability to counter

[15] Elina Noor, “Positioning ASEAN in Cyberspace,” Asia Policy 15, no. 2 (2020): 2.
[16] Candice Tran Dai and Miguel Alberto Gomez, “Challenges and Opportunities for Cyber Norms in ASEAN,” 3, 3, no. 2 (2018): 217–35; Noor, “Positioning ASEAN in Cyberspace,” 107–14.
[17] Noor, “Positioning ASEAN in Cyberspace,” 107-108.
[18] T. W. Feakin, L. Nevill, and Z. Hawkins, *Cyber Maturity in the Asia-Pacific Region*, ed. 2016; Tran Dai and Gomez, “Challenges and Opportunities for Cyber Norms in ASEAN,” 228–29.

China in the immediate future. In addition to overcoming ASEAN's cultural aspects, the region's cyber maturity varies considerably, making a singular approach for cyber ineffective.[19]

Cyber (digital) maturity is the idea that every country has a varying degree of development in "ICT, adoption of digital products and services, as well as growth of the digital economy."[20] This measure of maturity, along with political regime type, correlates to whether a nation is likely to engage in more significant cyber issues and how they might address them (see Appendix for complete description).[21] Elina Noor from the Asia-Pacific Center for Security Studies agrees and suggests that "not all ASEAN member states have the requisite legal, technical, or judicial capacity to prosecute cyber-related offenses."[22] Thus, it is in the United States' best interest to find additional ways to counter China's actions that are supportive of ASEAN, but at a faster rate and willingness then its natural tendencies allow. Bilateral, military cyber partnerships are the best way to counter China's actions.

INDIVIDUALIZED BILATERAL COOPERATION

Individual relationships with influential nations in the region will be the most effective and fastest way to counter China's provocations. In the short term, the United States and individual partners can share different skills and techniques and support digital capacity building where "both the donor and beneficiary states learn from each other."[23] If the United States fails to fill that void, China absolutely will considering China is physically closer and regional nations are economically intertwined with China as it look to expand its Digital Belt Road Initiative.[24] Alarmingly, China's version of norms look to "bypass domestic restrictions on privacy,

[19] Fergus Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," 9-11.
[20] Tran Dai and Gomez, "Challenges and Opportunities for Cyber Norms in ASEAN," 222.
[21] Tran Dai and Gomez, "Challenges and Opportunities for Cyber Norms in ASEAN," 220-222.
[22] Adam Segal et al., "The Future of Cybersecurity Across the Asia-Pacific," *Asia Policy* 15, no. 2 (2020) 57-59.
[23] Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," -Accessed 27 September 2020; Noor, "Positioning ASEAN in Cyberspace," 114.
[24] Poh and Ong, "PLA Reform, a New Normative Contest, and the Challenge for ASEAN," 127.

democracy, and transparency, which are Western normative standards."[25] To help advance regional and global cyber norms, the United States needs to partner with the right nations to effectively use cyberspace against China in the South China Sea.[26] This appraoch supports USCYBERCOM's "defend forward" strategy.[27] The idea is to seek out the adversary in gray space, not just sit in a [cyber] defensive posture and wait. Additionally, cyber-attacks become less effective as information about the malware or attack vector is shared.[28] Therefore, open dialogue, strategic cyber relationships, and persistent engagements are critical to combatting any adversarial cyber actor. Bilateral engagements focused on confidence-building measures, information sharing, and best practices are crucial to protecting the United States and its partners from further exploitation by Chinese cyber-attacks.

COUNTRY ANALYSIS AND RECOMMENDATIONS

Bilateral cooperation with any ASEAN nation would provide a mutually beneficial partnership with the United States to counter China's cyber tactics. However, due to finite budgets and limited high-demand, low-density practitioners, certain countries in ASEAN lend themselves more advantageous, individual partnering where the United States could be the most effective. When one evaluates the individual nations against cyber maturity, territorial claims, and current U.S. relations, Singapore, Vietnam, and the Philippines are the best candidates to establish immediate military cyber cooperation partnerships.

Singapore is a cybersecurity powerhouse and shares a similar vision to the United States regarding cyber policy and cyber norms. According to the International Cyber Policy Center in 2017, Singapore was the most digitally mature nation in ASEAN and third in the entire Asia-

[25] Poh and Ong, "PLA Reform, a New Normative Contest, and the Challenge for ASEAN," 116.
[26] Noor, "Positioning ASEAN in Cyberspace," 110.
[27] Nakasone and Sulmeyer, "How to Compete in Cyberspace."
[28] Nakasone and Sulmeyer, "How to Compete in Cyberspace."

Pacific region, even surpassing China.[29] Singapore developed a cybersecurity strategy and created a national level Cyber Security Agency.[30] During its 2018 regional ASEAN chairmanship, Singapore established the ASEAN Cyber Capacity Program and the ASEAN-Singapore Cyber Center of Excellence. "The center's focus on training, research, and information exchange on strategy, policy, legislation, and operations related to cyberspace was deliberately designed to align cyber diplomacy efforts with operational issues. This, in turn, facilitates regional coordination toward a unified perspective on international platforms."[31] Therefore, Singapore is an advocate and regional leader in cyberspace and declared that it is "committed to strong international collaboration for our collective global security. Singapore will actively cooperate with the international community, particularly ASEAN, to address transnational cybersecurity and cybercrime issues."[32] The United States military should move urgently to establish more technical level relationships with the "inclusion of cyber operators [...] who actually do the hacking in bilateral dialogues."[33] Additionally, since Singapore does not currently hold any territorial claims to the South China Sea, China is likely to see a robust cyber relationship with Singapore much less provocatively than others. For these reasons, Singapore is the best candidate for immediate, bilateral military cybersecurity cooperation.

Like Singapore, Vietnam is equally poised to have a mutually beneficial military cyber relationship with the United States. First and foremost, Vietnam is the 2020 ASEAN chair, which provides an excellent opportunity to support ASEAN's long-term goals while focusing on a bilateral partnership in the near-term. Lower than Singapore, Vietnam ranked fourteenth on the

[29] Fergus Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," 9-11.
[30] Jayakumar, "Will there be One ASEAN Voice on Cyber?"
[31] Noor, "Positioning ASEAN in Cyberspace," 113.
[32] "Singapore's New Cybersecurity Strategy Announced." *SMB World Asia (Online)* (2016).
[33] Alex Grigsby, "The End of Cyber Norms," 59, no. 6 (2017) 109-122.

2017 cyber maturity report but has matured quickly since the reports publishing and since its 2018 Law on Cybersecurity. "By the end of January this year, Vietnam had 68.17 million Internet users, accounting for 70% of the population."[34] With rapid economic and digital growth and a vision of bringing Vietnam into the 50 leading countries on the United Nations E-Government Development Index, there are equally as many opportunities for cyber threats, thereby making cybersecurity a top national priority.[35] Vietnam is also navigating a hotly contested territorial claim against China in the South China Sea and is subject to China's bullying tactics.[36] Since we know China will continue to use cyber for retaliatory actions against nations, Vietnam would be of particular importance for a bilateral relationship with the United States.

One other factor that is different from Singapore is that a military cyber relationship provides additional thawing of relations between the United States and Vietnam in the post-Vietnam War era. The United States has made tremendous progress in its relationship with the former adversary. However, confidence-building measures in cyber provide an excellent opportunity to solidify the renewed relationship below the strategic level and break down any lingering wariness. Events such as "training, exercises, and exchanges can serve to build critically important personal relationships among current and rising defense and political leaders and represent promising, often low-cost investments that two or more actors make in each other."[37] However, some opponents argue that Vietnam's authoritarian regime's desire to internally control the Internet and focus on offensive cyber with tactics mimicking China

[34] "MIL-OSI Asia Pacific: Vietnam, Singapore Boost Cooperation on Cybersecurity."
[35] "MIL-OSI Asia Pacific: Vietnam, Singapore Boost Cooperation on Cybersecurity."
[36] Fergus Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," 9-11.
[37] Harold et al., *The Thickening Web of Asian Security Cooperation: Deepening Defense Ties Among U.S. Allies and Partners in the Indo-Pacific*, 349–350.

Advanced Persistent Threats (APTs) should keep the United States from considering Vietnam for further partnership.[38] Nevertheless, if Vietnam is committed to its eCommerce transformation, then “stricter internet control [will] dampen innovation and impact the growth of Vietnam's digital economy and its competitiveness,” and that does not appear to be something Vietnam is willing to risk.[39] The United States also needs to be willing to take some risk. An opportunity to partner with a nation that behaves similarly in the cyber domain to one of the United States’ most significant competitors will allow operators to gain insight into resemblances and threats that can be equally as detrimental to the United States. if not defended against quickly.

Like Vietnam, the Philippines offer an opportunity for the United States to bolster a moderately mature digital partner with Chinese contested territorial claims to the South China Sea and is susceptible to bullying tactics. In terms of cyber maturity, the Philippines is right behind Vietnam. In 2019, experts projected that the Philippine digital economy would expand more than 250 percent from $7 billion in 2019 to $25 billion by 2025, providing plenty of attack surface for Chinese hackers.[40] Philippines lays claims to the Scarborough Shoal and the Spratly Islands in the South China Sea, but its public discontent with China caused the Philippines to be a repeat target of Chinese cyber-attacks. In 2012, China and the Philippines were involved in mutual cyber-attacks that surrounded their island disputes.[41] An attack followed this in “August 2016 called the South China Sea Remote Access Trojan program, where hackers extracted confidential information from the Philippines' Department of Justice and the major international law firm that represented nation-states” at the Permanent Court of Arbitration for the territorial

[38] Tran Dai and Gomez, “Challenges and Opportunities for Cyber Norms in ASEAN,” 228–29.

[39] Nguyen Phuong, "The Truth about Vietnam’s New Military Cyber Unit," *Diplomat (Rozelle, N.S.W.)* (2018).

[40] "PHL Digital Economy seen at $25 Billion in 2025." *Business Mirror,* 2019.

[41] Mark Manantan, "The Cyber Dimension of the South China Sea Clashes," *Diplomat (Rozelle, N.S.W.)* (2019).

disputes.[42] In April 2020, a Chinese cyber-espionage group deployed two malicious software variants that targeted government and private organizations in the Philippines, which corresponded to the “20-year negotiation between the Philippines and Indonesia on their maritime boundary treaty.”[43] The timing and tempo of such attacks should be of immediate concern to the Philippines and partner nations alike.

Lastly, the United States should consider a tactical cyber relationship as a method to repair the Philippines' strained relationship since President Duterte took office. If escalations with China take the United States to the point of armed conflict, locations from which to power-project in Southeast Asia will be of strategic importance. The Philippines is a critical location for United States operations. The United States is in an excellent position to use a bilateral cyber relationship to restore ties with the Philippines while offering them recent cyber technology and an opportunity to protect themselves from revisionist China.

CONCLUSION

An emboldened China continues to increase it cyber-attacks against nations in the South China Sea. “Knowing that China's approach toward the South China Sea has never relied on one-dimensional or oversimplified tactics,” the United States and ASEAN partners can expect that China will evolve its approach to “cement its unilateral control of the resource-rich stretch waters” by continuously increasing cyber-attacks.[44] Despite ASEAN's progress in the cyber domain, cultural limitations make such progress insignificant compared to the speed of China’s attacks. The DoD needs to focus on rapidly increasing bilateral cyber relationships within the region while supporting long-term goals for international cyber norms. Therefore, to secure the

[42] Manantan, "The Cyber Dimension of the South China Sea Clashes."
[43] Manantan, "The Cyber Dimension of the South China Sea Clashes."
[44] Manantan, "The Cyber Dimension of the South China Sea Clashes."

global commons and ensure freedom of navigation through cyber, the United States military should immediately invest in bilateral cyber relationships with Singapore, Vietnam, and the Philippines. Doing so will ensure the United States and its bilateral partners increase its resiliency against Chinese tactics, grow emerging relationships in cyber, and ultimately deter China from its continued predatory actions in the South China Sea.

BIBLIOGRAPHY

“ASEAN Chair - ASEAN: ONE VISION ONE IDENTITY ONE COMMUNITY.” ASEAN. Accessed 27 September 2020. https://asean.org/asean/asean-chair.

"How Estonia Became a Global Heavyweight in Cyber Security." Accessed 27 September 2020. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

"MIL-OSI Asia Pacific: Vietnam, Singapore Boost Cooperation on Cybersecurity." Accessed 27 September 2020. https://global.foreignaffairs.co.nz/2020/09/30/mil-osi-asia-pacific-vietnam-singapore-boost-cooperation-on-cybersecurity/.

"PHL Digital Economy seen at $25 Billion in 2025." *Business Mirror,* 2019, Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV09T8MwED3RdmGiCBCflQfWtIntOPGEoGrVAaG2qlQ6VXZsVx1wv4X499hpAqgMDIxRMsQ53_M7x-8eAMHNMDjABCFwxIzJ-UesDHGcTmjMEs3SLNTGS4nbY_I6SAcTPiwOF3ppTBHuEiVz6FaLzO-atzAh3jiGM_qwXAXeR8r_by1MNSpQc7mYpFWoPXVe-sNyjmHMMftBcfbXuTGPWxpdQRWl_Bcs52tN9wTKE7W7jX3PmnP19iWZPujh-K9Xr0PdA9xSLPUaPe7nzykcaXsGrX7vGan5zPuJIJ0rlz_QxhW8SGzRPY6R9Js0C4vmFmHHZs5h1O2M2r2gMFYIZiyhAXE1o5EuubFIpKFxKGiY-c5tSmYyFO4mVZFmmTIq5YZrKaRMuYqUb7xDY00uoGoXVl8CkoyFJIsNk5hTIbE0ihBBtctsR5RkegWN8gNMbTmozfR7_Nd_PXADx46jcC__i_AtVLfrnb6DWh6CBlSS8aRRhPgT04G17w.

"Significant Cyber Incidents | Center for Strategic and International Studies." Accessed 27 September 2020. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

"Singapore: Cyber Security Predictions for 2017: An Asia-Pacific Perspective, According to Frost & Sullivan." *MENA Report* (2016a): Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1863169533%3Faccountid%3D322.

Singapore’s Cybersecurity Strategy: APT811 Design & Innovation Agency, 2016b. Accessed 27 September 2020. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

"Singapore's New Cybersecurity Strategy Announced." *SMB World Asia (Online)* (2016c): Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1827858130%3Faccountid%3D322.

"Targeted Cyber Attacks to Infiltrate Nations Around South China Sea." *Enterprise Innovation* (2015): Accessed 27 September 2020.

https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1682500353%3Faccountid%3D322.

"U.S. Department of State, Bilateral Relations Fact Sheet." Accessed 27 September 2020. https://www.state.gov/.

"United States, Vietnam: ASEAN, U.S. Release Joint Statement on Cybersecurity Cooperation." *MENA Report* (2018). Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2134504801%3Faccountid%3D322.

"Vietnam: Vietnam to Improve Cyber Security." *Asia News Monitor,*2019b. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2211918446%3Faccountid%3D322.

Cho, Yoonyoung and Jongpil Chung. "Bring the State Back in: Conflict and Cooperation among States in Cybersecurity." *Pacific Focus* 32, no. 2 (2017): 290-314. Accessed 27 September 2020. https://onlinelibrary-wiley-com.usnwc.idm.oclc.org/doi/epdf/10.1111/pafo.12096

CISA. "ICS Alert (IR-ALERT-H-16-056-01)
Cyber-Attack Against Ukrainian Critical Infrastructure." Accessed 27 September 2020. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

Clemens,Walter C.,,Jr. "Cyber and Other Powers in Asia." Asian Perspective 43, no. 3 (Summer, 2019): 585-592. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2282990235%3Faccountid%3D322.

Cordesman, Anthony H. *China's New 2019 Defense White Paper*: Center for Strategic and International Studies, 2019. Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0EUrExJTktKAdVWSJbC5n2oC7DoD01KSBeiehzTDtBRz0L5h53DjiECLwEjLIOjiQtDWGGh0w0pJcNGdkp8MGjXXBzYczM1MjYA1oH1BoS7oHinQfCv0Ug1mBlYj0DFHLAysLgHB_mEYRS24_nATYICtki0tzitP1stMyYVvg0Y7l5Ei5wgysEEa1EIMTKl5Igwq4Nux1YsVgEWZArAOtlRwSU0D9ltTFcD34ikEJBakFokyaLi5hjh76MLsiwdGPWg8PzEvNb-0OB5ho7EYA0tefl6qBINCErAKNjJNSjEHtmVMUpJTLU1SjdJMDUxSzAzNgK0rC0kGRYLGSRGhRpqBC-Ru0DCnkYkMA0tJUWmqLAMrOBjloIEOAEscm8A.

Department of Defense. Summary of the 2018 DoD Cyber Strategy. Washington, DC: Department of Defense, 2018. Accessed 27 September 2020. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Department of Defense. Summary of the 2018 National Defense Strategy of the United States of America. Washington, DC: Department of Defense, 2018. Accessed 27 September 2020. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Engstrom, Jeffrey. *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*: RAND Corporation, 2018. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2010633848%3Faccountid%3D322.

Feakin, T. W., L. Nevill, and Z. Hawkins. *Cyber Maturity in the Asia-Pacific Region*, 2016, 12 December 2017, Accessed 27 September 2020. https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017.

Glosserman, Brad. *ARF to the Forefront: Promoting Cybersecurity CBMs in the Asia-Pacific: A Conference Report of the CSCAP Workshop on Cybersecurity in the Asia-Pacific*. Honolulu, United States Honolulu, Honolulu: Center for Strategic and International Studies (CSIS), 2017. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1902435240%3Faccountid%3D322.

Gomez, Miguel Alberto. "Awaken the Cyber Dragon: China's Cyber Strategy and its Impact on ASEAN." *Journal of Communication and Computer* 10, (June 30, 2013): 796-805.

Greiman, Virginia. *Navigating the Cyber Sea: Dangerous Atolls Ahead*. Reading, United Kingdom Reading, Reading: Academic Conferences International Limited, 2019. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2198531195%3Faccountid%3D322.

Grigsby, Alex. "The End of Cyber Norms." 59, no. 6 (2017): 109-122. Accessed 27 September 2020. doi:10.1080/00396338.2017.1399730. https://doi-org.usnwc.idm.oclc.org/10.1080/00396338.2017.1399730.

Grossman, Derek. "Can Vietnam's Military Stand Up to China in the South China Sea?" Asia Policy 13, no. 1 (01, 2018): 113-134. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2002001862%3Faccountid%3D322.

Hanson, Fergus, Tom Uren, Fergus Ryan, Michael Chi, Jack Viola, and Eliza Chapman. *Cyber Maturity in the Asia Pacific Region 2017*: International Cyber Policy Centre, 2017. Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV1La8MwDBZj3WG3vd_ge0hJm-bRwwajbPS2tWvZdjJ52COHetC0jP77SbFbNz2MrbCLCSKOP8WKJSuSDOC3m567sSagEoxiGYZpil9mlqW-L0QYSlJvuSclJSf3Xv23QTx47w7tEaGW9q8TjzScekqk_cPkrx6KBLxGEcAWhQDbn8XAFB9YpGLqTKh6J5nbJqgRcSSOCcdz6GgGFAFU0VYlienHvHT6CWWGWT_0xBmvZY6Zm4YLK18mBp_iO9a9Ca1ow5tQd0NqjLpAsfY2C6s2lr_K75-f6sRKORaKIz-c-OGGH6754TQsb7VxOxxy6kw1zid5kc1uhXLHL1SIIAijWkWDStmPDmBP70oOYUeoIziroWWr6MFjaFbI2fLtskIxRMMIDTNomEbDCM0J3D0-jHp9l0bkVZlKUfLfs-

Cdwq76VOIcWC5jkXTypJt1MlwOg1SiQYomp5AxWr5RcAHRloNcbt3zCvbtVF9DQ6JsixtozEv1lX0DBPQzhA.

Harold, Scott W., Derek Grossman, Brian Harding, Jeffrey W. Hornung, Gregory Poling, Jeffrey Smith, and Meagan L. Smith. *The Thickening Web of Asian Security Cooperation: Deepening Defense Ties among U.S. Allies and Partners in the Indo-Pacific*. RAND Corporation, 2019. Accessed 27 September 2020. doi:10.7249/RR3125. https://www.rand.org/pubs/research_reports/RR3125.html.

Hjortdal, Magnus. "China's use of Cyber Warfare: Espionage Meets Strategic Deterrence." Journal of Strategic Security 4, no. 2 (2011): 1-24. Accessed 27 September 2020. doi:http://dx.doi.org.usnwc.idm.oclc.org/10.5038/1944-0472.4.2.1. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F2205357719%3Faccountid%3D322.

Jayakumar, Shashi. "Will there be One ASEAN Voice on Cyber?" Newstex. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2253823883%3Faccountid%3D322.

Kemburi, Kalyan M. and Mingjiang Li. *New Dynamics in US-China Relations: Contending for the Asia Pacific*. London: Routledge, 2015. Accessed 27 September 2020. http://usnwc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=873038&site=ehost-live.

Kofman, Michael, Olesya Tkacheva, Jenny Oberholtzer, Andrew Radin, Brian Nichiporuk 1966, Katya Migacheva, United States. Department of the Army. Deputy Chief of Staff, G-8, Arroyo Center. Army Research Division, Rand Corporation, and Arroyo Center. Strategy, Doctrine,and Resources Program. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Vol. no. 1498. Santa Monica, CA: Rand Corporation, 2017. Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwdV3PS8MwFH7odvHmj4o_pryTnjZm067pxYOlw4M4VnXV00iaDESIw1rH_ntf0lJF3KWQEtI2ecnL95r3fQDMHwz7f9YEHmoaaB3b_2JSSZ8gt1QFOaPhVSGFk5BMcvY85dOXOPtRLjXia1UMHH53SH0zpm8FrOuDlTQP2ShoSH7bo1_pzUOazdJsG7qE3UOr9HCfJ21Ihl4qjALuWCIJ5tu9fcMK1ZYjy35dmlXxywmNd6GrbWbCHmxpsw9eTfCxxgu07LHCKfSuD-D6jtYuMiW0iSOYVWTz4rLEyVLXY13iq0Er5qUFCqMwFY4qAZ_erFiE9qA3Th-T2757_ryJ7syr-lPZIXTMu9FHgMynbYCMQxmpRSACJflouKBanGlCX4ofg_dvEycb7p_Cjm99mYs79KDz-VHps6Ybzl0P0nU2yb8BOReLTQ.

Levitsky, Steven and Lucan Way 1968. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. New York: Cambridge University Press, 2010. Accessed 27 September 2020. https://www-cambridge-org.usnwc.idm.oclc.org/core/journals/perspectives-on-politics/article/competitive-authoritarianism-hybrid-regimes-after-the-cold-war-by-steven-levitsky-and-lucan-a-way-new-york-cambridge-university-press-2010-517p-9500-cloth-2999-paper/E04BC197BD8336D27859AB8B63626AE2.

Liu, Yangyue. "Crafting a Democratic Enclave on the Cyberspace: Case Studies of Malaysia, Indonesia, and Singapore." *Journal of Current Southeast Asian Affairs* 30, no. 4 (2011): 33-55. Accessed 27 September 2020. https://journals.sagepub.com/doi/pdf/10.1177/186810341103000402.

Manantan, Mark. "The Cyber Dimension of the South China Sea Clashes." *Diplomat (Rozelle, N.S.W.)* (2019). Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwpV1NT4NAEJ1YuHiqHzV-NuvFeKEKSxc4GcU2xkNjWxPrqVlgiR4ELRLDv3dmC5rUgybeCZnsvLx9uzszD4A7vXNrhRNiRyCQeSpjPDTbfpIQdKSf2gr1h5DU7xw-8NnYHz8Gk7q4kFpj6nQ3LKmpO8ljujU_Q2WCakO4gXfx-maRjxS9t9amGi0wcfPq-waYV4PR3aRhZ7fvaf8ROgZZIvBmPzhYbyzDNjTls2WRfcS95-Tlqz96ZWDjv-LcgHYzSZpdLrGyCWsq24LOck5IxU4YDaGV2ui32gYH8cPCKlILdk0GAHSpxvKUoV5k2naPaedtNlWSkbHmkyo6cDoc3Ic3VhPfHDFEDwMyU3lZzL8j5DtgZHmmdoEJX6H447ZIU-o2xWxJL4p4IkQguRc5e3D86-_2__DNAayjCAl0UZ17CMb7olRHYOpl79bZ60Jrejv6BJWOszE.

Mohan, Rakshit and Aditya Laxman Jakki. "Sovereignty Issues in the South China Sea: The Republic of the Philippines Vs the People's Republic of China." *Maritime Affairs: Journal of the National Maritime Foundation of India* 15, no. 2 (2019): 15-30. Accessed 27 September 2020. https://www.tandfonline.com/doi/abs/10.1080/09733159.2020.1711584.

Nakasone, Paul M. and Michael Sulmeyer. "How to Compete in Cyberspace." 25 August 2020, Accessed 27 September 2020. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Nguyen The Phuong. "The Truth about Vietnam’s New Military Cyber Unit." *The Diplomat,* 2018. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1985921974%3Faccountid%3D322.

Noor, Elina. "Positioning ASEAN in Cyberspace." *Asia Policy* 15, no. 2 (2020): 107-114. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2399206722%3Faccountid%3D322.

Pesek, William. "Making Sense of the South China Sea Dispute." *Forbes Asia,* 22 August 2017. Accessed 3 October 2020. https://www.forbes.com/sites/outofasia/2017/08/22/making-sense-of-the-south-china-sea-dispute/#eaf73be1c3b9.

Phuong, Nguyen. "The Truth about Vietnam’s New Military Cyber Unit." *Diplomat (Rozelle, N.S.W.)* (2018). Accessed 27 September 2020. http://usnwc.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0EUrEwzNzIFRbWhobG5hkmaaDNr_aGmaCtrXmJyYnGQB2pzsHG4cEWgRGGkZBF1cCNoaA41uWCkJLrpT8pNBo-b6wO6yqSUww5mb2BcU6oLukQLNt0Iv1WBmYAVWXqYWLAysTq5-AUGw0tnE1Bx8_wioG6RrZmkegVEGgysWNwEG2PLZ0uK88mS9zJRc-

P5otAMbKXKnIIMA7CRpBUdIWhFiYErNE2YQhZwTUqmgpgA6hDYRfNFvpQiDMTD9KIQUlZZkKIBmhkoUwjJTS_IScx81zCxWAJaMCr7g472BGp0rk1KLFEBtV1EGDTfXEGcPXZgD44GJCDQzkJiXml9aHI9worEYA0tefl6qBINCsoFlMrC9Y2mYZpgM7KQkJSWnWFqappmbGySaGySbm0kyKBI0TooINdIMXMBWiAV4XMNShoGlpKg0VZaBFRzuctDok2NgDvbyAwC6LrTX.

Poh, Angela and Weichong Ong. "PLA Reform, a New Normative Contest, and the Challenge for ASEAN." *Asia Policy* 14, no. 4 (2019): 107-128. Accessed 27 September 2020. https://search-proquest-com.usnwc.idm.oclc.org/docview/2312463283/fulltextPDF/4A61AF19487F481CPQ/1?accountid=322

Segal, Adam. "China's Pursuit of Cyberpower." *Asia Policy* 15, no. 2 (2020): 60-66. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrt_apr2020.pdf#:~:text=China%E2%80%99s%20Pursuit%20of%20Cyberpower%20Adam%20Segal%20C%20hina,conducted%20to%20strengthen%20the%20competitiveness%20of%20China%E2%80%99s%20economy%2C.

Segal, Adam, Valeriy Akimenko, Keir Giles, Daniel A. Pinkston, James A. Lewis, Benjamin Bartlett, Hsini Huang, and Elina Noor. "The Future of Cybersecurity Across the Asia-Pacific." *Asia Policy* 15, no. 2 (2020): 57-59. Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2399206603%3Faccountid%3D322.

Storey, Ian. "Assessing the ASEAB-China Framework for the Code of Conduct for the South China Sea." *ISEAS Yusof Ishak Institute* 62, no. 2017 (8 August 2017): 1-7. Accessed 27 September 2020. https://www.iseas.edu.sg/wp-content/uploads/2018/02/ISEAS_Perspective_2017_62.pdf.

Tran Dai, Candice and Miguel Alberto Gomez. "Challenges and Opportunities for Cyber Norms in ASEAN." 3, no. 2 (2018): 217-235. Accessed 27 September 2020. doi:10.1080/23738871.2018.1487987. https://doi.org/10.1080/23738871.2018.1487987.

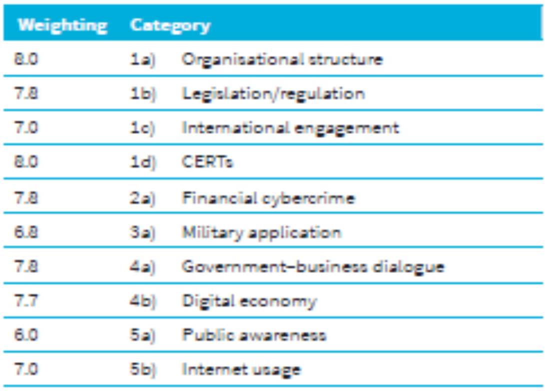
Vasagar, Jeevan and Leo Lewis. "Chinese Hackers Shift Focus to Asia After US Accord." *FT.Com* (2017): Accessed 27 September 2020. https://login.usnwc.idm.oclc.org/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdocview%2F1902715607%3Faccountid%3D322.

Vavra, Shannon. "Suspected Chinese Hackers Aim Attacks at Vietnamese Government Officials." Accessed 27 September 2020. https://www.cyberscoop.com/south-china-sea-maritime-hacking-vietnam/.

APPENDIX – CYBER MATURITY

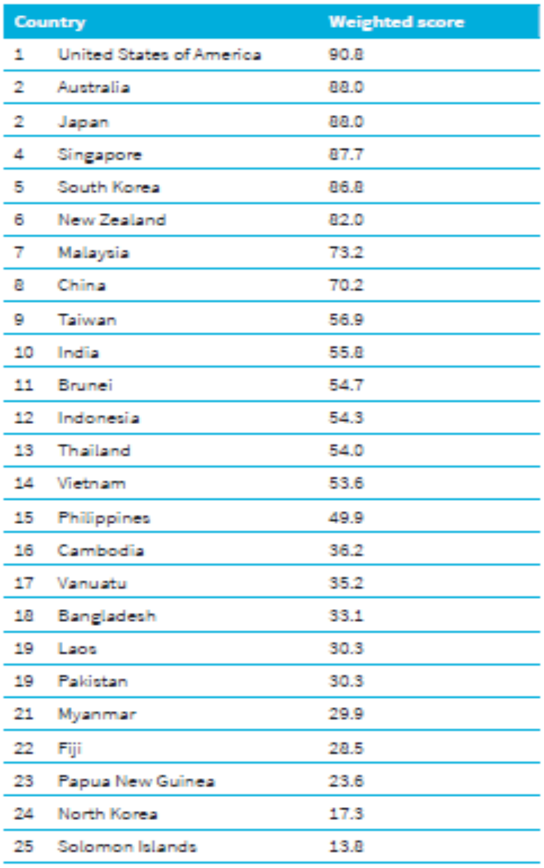
Below is an extract from Cyber Maturity in the Asia Pacific Region 2017 Report, published by the International Cyber Policy Centre from the Australian Strategic Policy Institute. It outlines the weighting of each category considered (Table 1) and the weighted scores for each country (Table 2).[45] Page 2 give a detailed description of each weighted factor. Table 3 represents the author's data compilation on which countries lend themselves to mutually beneficial, immediate bilateral cyber relationships.

TABLE 1: WEIGHTING ASSIGNED TO EACH CATEGORY, 2017



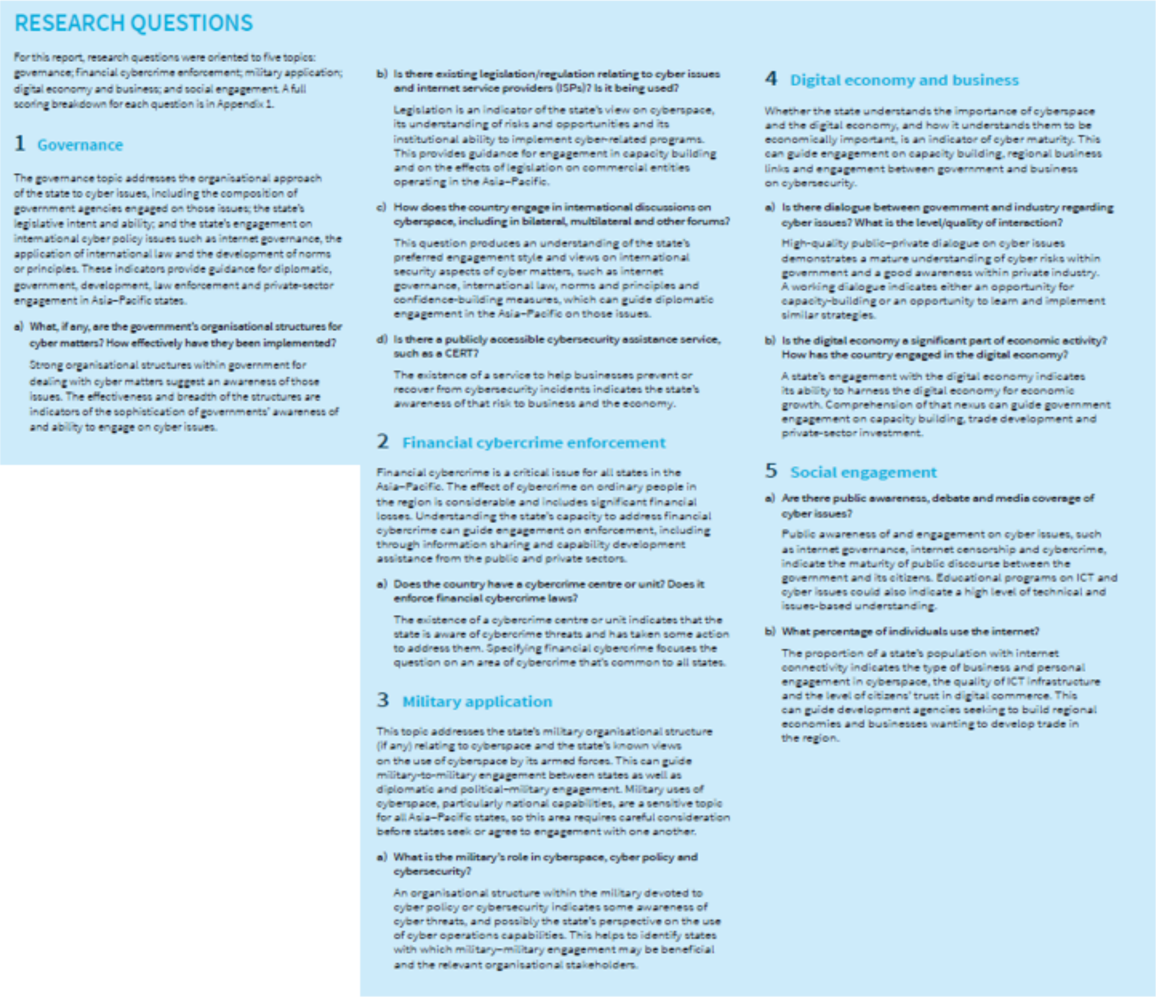
Weighting	Category	
8.0	1a)	Organisational structure
7.8	1b)	Legislation/regulation
7.0	1c)	International engagement
8.0	1d)	CERTs
7.8	2a)	Financial cybercrime
6.8	3a)	Military application
7.8	4a)	Government–business dialogue
7.7	4b)	Digital economy
6.0	5a)	Public awareness
7.0	5b)	Internet usage

TABLE 2: WEIGHTED SCORES, 2017



Country		Weighted score
1	United States of America	90.8
2	Australia	88.0
2	Japan	88.0
4	Singapore	87.7
5	South Korea	86.8
6	New Zealand	82.0
7	Malaysia	73.2
8	China	70.2
9	Taiwan	56.9
10	India	55.8
11	Brunei	54.7
12	Indonesia	54.3
13	Thailand	54.0
14	Vietnam	53.6
15	Philippines	49.9
16	Cambodia	36.2
17	Vanuatu	35.2
18	Bangladesh	33.1
19	Laos	30.3
19	Pakistan	30.3
21	Myanmar	29.9
22	Fiji	28.5
23	Papua New Guinea	23.6
24	North Korea	17.3
25	Solomon Islands	13.8

[45] Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," 9-11.



RESEARCH QUESTIONS

For this report, research questions were oriented to five topics: governance; financial cybercrime enforcement; military application; digital economy and business; and social engagement. A full scoring breakdown for each question is in Appendix 1.

1 Governance

The governance topic addresses the organisational approach of the state to cyber issues, including the composition of government agencies engaged on those issues; the state's legislative intent and ability; and the state's engagement on international cyber policy issues such as internet governance, the application of international law and the development of norms or principles. These indicators provide guidance for diplomatic, government, development, law enforcement and private-sector engagement in Asia–Pacific states.

a) What, if any, are the government's organisational structures for cyber matters? How effectively have they been implemented?

Strong organisational structures within government for dealing with cyber matters suggest an awareness of those issues. The effectiveness and breadth of the structures are indicators of the sophistication of governments' awareness of and ability to engage on cyber issues.

b) Is there existing legislation/regulation relating to cyber issues and internet service providers (ISPs)? Is it being used?

Legislation is an indicator of the state's view on cyberspace, its understanding of risks and opportunities and its institutional ability to implement cyber-related programs. This provides guidance for engagement in capacity building and on the effects of legislation on commercial entities operating in the Asia–Pacific.

c) How does the country engage in international discussions on cyberspace, including in bilateral, multilateral and other forums?

This question produces an understanding of the state's preferred engagement style and views on international security aspects of cyber matters, such as internet governance, international law, norms and principles and confidence-building measures, which can guide diplomatic engagement in the Asia–Pacific on those issues.

d) Is there a publicly accessible cybersecurity assistance service, such as a CERT?

The existence of a service to help businesses prevent or recover from cybersecurity incidents indicates the state's awareness of that risk to business and the economy.

2 Financial cybercrime enforcement

Financial cybercrime is a critical issue for all states in the Asia–Pacific. The effect of cybercrime on ordinary people in the region is considerable and includes significant financial losses. Understanding the state's capacity to address financial cybercrime can guide engagement on enforcement, including through information sharing and capability development assistance from the public and private sectors.

a) Does the country have a cybercrime centre or unit? Does it enforce financial cybercrime laws?

The existence of a cybercrime centre or unit indicates that the state is aware of cybercrime threats and has taken some action to address them. Specifying financial cybercrime focuses the question on an area of cybercrime that's common to all states.

3 Military application

This topic addresses the state's military organisational structure (if any) relating to cyberspace and the state's known views on the use of cyberspace by its armed forces. This can guide military-to-military engagement between states as well as diplomatic and political–military engagement. Military uses of cyberspace, particularly national capabilities, are a sensitive topic for all Asia–Pacific states, so this area requires careful consideration before states seek or agree to engagement with one another.

a) What is the military's role in cyberspace, cyber policy and cybersecurity?

An organisational structure within the military devoted to cyber policy or cybersecurity indicates some awareness of cyber threats, and possibly the state's perspective on the use of cyber operations capabilities. This helps to identify states with which military–military engagement may be beneficial and the relevant organisational stakeholders.

4 Digital economy and business

Whether the state understands the importance of cyberspace and the digital economy, and how it understands them to be economically important, is an indicator of cyber maturity. This can guide engagement on capacity building, regional business links and engagement between government and business on cybersecurity.

a) Is there dialogue between government and industry regarding cyber issues? What is the level/quality of interaction?

High-quality public–private dialogue on cyber issues demonstrates a mature understanding of cyber risks within government and a good awareness within private industry. A working dialogue indicates either an opportunity for capacity-building or an opportunity to learn and implement similar strategies.

b) Is the digital economy a significant part of economic activity? How has the country engaged in the digital economy?

A state's engagement with the digital economy indicates its ability to harness the digital economy for economic growth. Comprehension of that nexus can guide government engagement on capacity building, trade development and private-sector investment.

5 Social engagement

a) Are there public awareness, debate and media coverage of cyber issues?

Public awareness of and engagement on cyber issues, such as internet governance, internet censorship and cybercrime, indicate the maturity of public discourse between the government and its citizens. Educational programs on ICT and cyber issues could also indicate a high level of technical and issues-based understanding.

b) What percentage of individuals use the internet?

The proportion of a state's population with internet connectivity indicates the type of business and personal engagement in cyberspace, the quality of ICT infrastructure and the level of citizens' trust in digital commerce. This can guide development agencies seeking to build regional economies and businesses wanting to develop trade in the region.

[46]

[46] Hanson et al., "Cyber Maturity in the Asia Pacific Region 2017," 9-11.

Table 3: Combined Data on Maturity, Territorial Claims, and Status of U.S. Relations

ASEAN Member (Most recent year as Chair) [47]	Cyber Maturity [48]	Territorial Claim [49]	Current Status of U.S. Relations [50]	Additional Factors
Singapore (2018)	87.7	No	Expansive and enduring; US is largest foreign investor	Regional Leader in Cybersecurity;
Malaysia (2015)	73.2	Yes	Moderate/expanding; 18th largest trading partner	
Brunei (2013)	54.7	Yes	Moderate; stable	
Indonesia (2011)	54.3	No	Moderate; stable	
Thailand (2009)	54.0	No	Key U.S. Ally; 20th largest trading partner	
Vietnam (2010)	53.6	Yes	Rapidly expanding; fastest growing exports for both countries	recent thawing of relations; authoritarian regime
Philippines (2006)	49.9	Yes	Enduring, expanding; U.S. one of largest investors and third largest trading partner	Critical geostrategic position and long-time partner; recent UNCLOS ruling against China
Cambodia (2012)	36.2	No	Minimal; expanding	
Laos (2016)	30.3	No	Minimal	
Burma (2014)	29.9	No	Minimal	

[47] Association of South East Asian Nations, “ASEAN Chair,” Association of South East Asian Nations.
[48] Hanson et al., “Cyber Maturity in the Asia Pacific Region 2017,” 9-11.
[49] William Pesek, "Making Sense of the South China Sea Dispute," *Forbes Asia,* 22 August 2017.
[50] "U.S. Department of State, Bilateral Relations Fact Sheets."