From Rizal Sukma and Yoshihide Soeya, eds., *Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance* (Tokyo: Japan Center for International Exchange, 2015)

9

Strategic Governance of Cyber Security: Implications for East Asia

ELINA NOOR

THIS CHAPTER ASSESSES the strategic challenges of security in cyber space in East Asia and outlines avenues for cooperation between ASEAN and Japan in this domain. For the purposes of defining the scope of the discussion, a number of parameters are offered at the outset. First, East Asia will refer to the 10 countries in Southeast Asia reflected in the ASEAN grouping as well as its northern neighbors of Japan, China, and the two states on the Korean peninsula. Second, cyber space will be loosely defined as the interconnected network of information technology infrastructures—including hardware such as fiber optic cables, computers, and mobile devices, as well as the Internet—that all allow for a flow of information and interactions between people.[1] Third, in referring to cyber security, this chapter will not be concerned with cyber crime (for example, phishing, spamming, or data misuse) or its technical solutions; instead, it will focus on a state's ability to protect and defend its critical national information infrastructure (CNII) at the strategic, policy level against an attack. Relatedly, it will explore the conduct of international relations between states in the virtual realm and question whether the existing framework of international law can be transposed and/or extended to cyber space, particularly if breaches in this domain threaten actual damage and destruction in the physical realm. In short, this will be referred to as "strategic cyber security."

This chapter is divided into four parts. The first will outline the strategic imperatives of cyber security for nations in general and for the ASEAN region in particular. The second will document how, despite the fact that awareness of cyber security and related civilian technical initiatives are increasingly gaining ground among governments in Southeast Asia, a strategic approach toward protecting and defending CNII continues to lag, both nationally and regionally. The third will contend that this lack of proactive direction by governments in the region disadvantages them in shaping international norms and rules as they evolve, contributes to cyber insecurity nationally and regionally, and promotes two tiers of influence in the cyber domain, which in turn perpetuates distrust and invites power plays in the region at large. And the fourth and final part will propose ways in which ASEAN and Japan can work together to address these gaps and challenges, particularly as ASEAN moves toward consolidating its broadband corridor[2] and regional integration.

The Strategic Imperatives of Cyber Security

Cyber space is a network of interconnected digital systems and infrastructure with an expansive reach under seas, over land, and in the cloud(s). It is a parallel, virtual, and undifferentiated realm in which dynamic, intangible packets of data are continuously routed from one node to another. Reflective of the code that underwrites it, its binary nature is apparent in the civilian/military and public/private divides across which it cuts. For cost efficiency, much of the software that is readily available in the commercial market is simply tweaked rather than written especially for military use, while much of a nation's critical infrastructure—from electricity grids to financial systems—that supports both civilian and military realms is now digitally operated. At the strategic level, cyber space is emerging as a significant military domain in addition to the domains of air, land, sea, and, for some, space. With its potential as a disruptive—and potentially destructive—method and means of warfare, cyber space is being touted as an asymmetric leveler and force multiplier to conventional warfare.

As governments and populations increasingly rely on cyber space for their daily activities, traditional divides will grow even more fluid so that what takes place virtually will have physical consequences, and the rules that govern cyber space will have to evolve on par and at pace with technology. The speed at which technology has evolved and continues to do so, however, can be overwhelming. This, coupled with confounding jargon, ensures that discussions of cyber security are frequently confined to the technical level with little discussion at the strategic level, notably within Southeast Asia.

To be sure, priorities differ among countries in the region because of divergences in technological, human, and financial capabilities. Additionally, whereas technical bureaucrats have little problem sharing threat and other information with each other and actually work seamlessly together across the region, strategic sensitivities prevent the same level of cooperation among security and military agencies, and cyber commands are usually parked within nations.

Issues such as what recourse to action would be available if a country's emergency services, military installation, or power plant were disabled by malicious code delivered from across the border, or how attribution would even be determined so that an appropriate response could be taken make for awkward discussions. ASEAN member states, in particular, traditionally tend to avoid direct consideration of conflicts and their aftereffects. However, if connectivity and community are key to ASEAN's integration, then it must begin to contemplate the implications of connectivity on community in all its forms, extending beyond the physical to the virtual. This also necessitates debate on the governing framework that will underpin the increasingly prominent virtual domain and that will offer clarity of action in the event of crises. Importantly, ASEAN member states working together with their Northeast Asian neighbors will have to build the necessary trust to collaborate at the strategic level in cyber security before norms and rules from beyond the region overtake them or are foisted upon them.

A Strategic Approach toward Cyber Security?

Over the last decade, ASEAN awareness of cyber space and the need to secure it has matured from transient recognition to broader and more sustained rhetoric, action plans, and initiatives.[3] In part, this has stemmed from the fact that Internet penetration in the region has been rising steadily, with dramatic growth forecasted over the next five years in the region's emerging markets of Vietnam and Myanmar.[4] However, much of ASEAN's focus on security in cyber space has been directed toward combatting transnational crime and, increasingly, securing regional economic integration. Cyber crime and cyber terrorism, for example, featured prominently in various ASEAN declarations and communiqués on transnational crime in the aftermath of the 2001 terrorist attacks in the United States.[5] Since then, a drive to integrate the ASEAN community by 2015 has reshaped ASEAN's focus on security in cyber space.

Given that achieving economic prosperity as the basis for political stability has been an ASEAN priority since its inception, it is perhaps no surprise that ASEAN was the first region in the developing world to adopt a harmonized legal framework for e-commerce. Spurred by accelerated plans for regional integration through, among others, the ASEAN ICT Master Plan 2015 and the Master Plan on ASEAN Connectivity, Southeast Asia remains the most advanced developing region in implementing harmonized e-commerce laws.[6] Nine of the 10 ASEAN countries have laws related to electronic transactions, while 8 have laws concerned with cyber crime.[7]

Publicly available information shows that from 2011 to 2012, the number of countries operating national cyber security programs jumped by nearly 70 percent among the 193 UN member states. Whereas in 2011 only 68 countries had such programs, by August 2012 there were 114 countries that had developed a domestic cyber security agenda with 47 of those having a military component.[8] The number of Asian countries (39) with their own cyber security programs came in first—ahead even of European countries (38)—with all 4 Northeast Asian countries and every ASEAN country except for Laos possessing a cyber security program.[9]

Like the binary codes that underwrite the Internet, duality pervades cyber space. The transferability of skills and software, as well as the kinetic effects that cyber attacks can have challenge traditional divides between civilian and military, state and nonstate, private and public, physical and virtual, and national and regional/international. Advanced persistent threats, for example, which may be deployed either by a state entity or a group of hired individuals acting under state authority—thus blurring the divide between state and nonstate actor and even between civilian and military—pose a danger to economic and national security interests which themselves overlap on occasion. In particular, this may occur where Internet-enabled espionage tools are remotely installed in commercial organizations that maintain or service sensitive sectors such as defense or utilities.

Although attacks in cyber space usually incur some form of economic loss as opposed to actual kinetic damage or injury, hybrid attacks that affect the virtual and physical realms are a real and potentially destructive possibility. An attack that shuts down the communications systems for emergency services in the event of a terrorist bombing, for example, may compound the number of injuries if victims are unable to receive urgent medical attention in the immediate aftermath of the event.

Operational controls of CNII are usually kept separate from administrative controls, but technological advances and superior hacking skills may make inroads that enable the circumvention of this security measure.[10] Additionally, most CNII accommodates links between administrative and operational control systems and is connected to the public Internet.[11] Even air-gapped controls—physically isolated from unsecured networks—are vulnerable to the weakest link, the end user, and may be compromised by the physical insertion of an infected USB drive into the system, as demonstrated by the Stuxnet computer worm. (Disconcertingly, in tests conducted prior to its release, Stuxnet showed that a computer worm is in fact capable of reducing to rubble a replica of a nuclear centrifuge by wreaking havoc on its operational speed.)[12] Software, as revealed by the recent US National Security Agency leaks, is not the only source of malware. Hardware, it seems, may be manipulated to include "back doors" at the design or production stage that would allow the computer to access data undetected by its security software.[13] In some cases, this secret entrance(s) cannot even be sealed by switching off the hard disk or reinstalling the computer's operating system.

While countries in Northeast Asia have surged ahead in responding to these evolving challenges by crafting proactive cyber security programs and strategies as well as dedicated organizations to protect and defend their critical infrastructure, ASEAN member states remain hampered by the digital divide, limited human and financial capacity, and differing priorities accorded to cyber security policy. Nevertheless, governments in even less technologically advanced countries have begun to establish national computer emergency response teams (CERTs) or computer incident response teams (CIRTs) to respond to cyber attacks.[14]

While essential as a structured line of defense, CERTs/CIRTs are essentially reactive, although they do also perform a monitoring function. As pointed out above, within the ASEAN region, their establishment has primarily been driven by the imperative of offering a secure and stable environment for e-commerce to grow, as well as of combatting cyber crime. To be sure, security in cyber space is premised at the practical level upon tactical and technical responses to attacks. However, as ASEAN countries become increasingly dependent on the Internet and each other as a community through a shared broadband infrastructure, a coordinated, strategic, long-term approach to cyber security needs to be jointly developed beyond the narrow confines of trade and economics or transnational crime. Even the ASEAN Political-Security Community Blueprint places cyber security within these two contexts rather than anticipating how evolving threats may impact upon elemental precepts like state sovereignty and international law.

404 Not Found Error: Where is East Asia's Strategic Cyber Security Agenda?

One of the most contentious issues concerning cyber security relates specifically to the treatment of cyber attacks by international law. A state that suffers an armed attack from another is conditionally afforded recourse to self-defense measures under international law.[15] It is as yet unclear whether a state that suffers by way of a cyber attack, however, is given the same latitude.

A distributed denial of service (DDOS) attack that paralyzes a state's power grid, thereby causing widespread traffic accidents and utility meltdowns, arguably differs in gravity from a DDOS attack on a state's financial and banking systems that results in massive economic losses. While website defacements and disruptions are fairly common occurrences as an expression of political displeasure, no DDOS attacks aimed at critical infrastructure have been carried out or even threatened in Southeast Asia to date.[16] There have, however, been threats of economic disruption by the activist hacker ("hacktivist") group known as "Anonymous," which warned of financial losses for Singapore through "aggressive cyber intrusion."[17] Larger-scale cyber attacks have occurred in Northeast Asia, resulting in substantial financial damage and national security risks but no actual kinetic destruction.[18]

These threats and attacks give rise to several questions with international legal connotations. First, where foreign state entities are implicated or accused of involvement in cyber attacks against another sovereign state, as North Korea has been,[19] the applicability of international laws governing the threat or use of force is called into question. Would cyber attacks even meet the "threat or use of force" threshold delineated—but undefined—in Article 2(4) of the United Nations Charter?[20] If so, what criteria would they need to fulfill? Would physical injury or damage need to have been caused as a direct result of cyber attacks, or would a certain, substantial quantum of economic loss suffice?

Second, Article 2(4) of the UN Charter lays the groundwork for the applicability of Article 51, which allows self-defense measures to be taken by members of the UN against an "armed attack." The term "armed attack" remains undefined[21] and opens up the possibility of a broad-based interpretation within which cyber attacks could fall. If the perpetrator's intent is to specifically cause harm and the magnitude and effect of the attacks are significant enough (the level of which would also need to be qualified), then it may be possible for a cyber attack to be liberally interpreted as constituting an armed attack within the ambit of Article 51.[22]

Third, because the charter was drafted at a time when wars meant states being at conflict with each other—i.e., attacks could reasonably be anticipated and aggressors could easily be identified—it assumes a set of propositions that fit awkwardly in the context of cyber space. Even the concept of warfare in or through cyber space is academically controversial.[23] In cyber space, nonstate actors may sometimes act under state authority to conduct attacks or they may be motivated by nationalist sentiments to act on their own. Articles 2(4) and 51 of the Charter refer specifically to states and UN members respectively, which would seem to exclude nonstate actors from the charter's ambit. Further, what sort of self-defense measures are available to state victims if cyber attacks are instantaneous and unpredictable? Would these measures be limited to cyber tools or could states avail themselves of other kinetic options, as the United States has declared for itself?[24] Even if states were to take self-defense measures, what would their target(s) be, since attribution in cyber space is vastly problematic?

These multiple scenarios underlie the larger question of whether the existing framework of international law adequately applies to conflict—and the treatment of espionage—in or through the use of cyber space. Articles 2(4) and 51 of the charter form part of the jus ad bellum (law governing the resort to force) corpus. However, jus in bello, or the body of laws governing the actual conduct of war, are more comprehensive and detailed. These will not be discussed in this chapter due to space constraints. Suffice it to say, though, that for all the reasons described above, East Asia will need to seriously deliberate and contribute to the evolving discussion on the applicability of both these bodies of law to cyber space.

Despite the enormity of the matter and its implications for the international community, the conversation is being promulgated by only a few countries—predominantly the United States and, to a lesser extent, the United Kingdom, Australia, and a few countries in continental Europe. The future may be in Asia, but in cyber space, the present is being shaped elsewhere.

The Tallinn Manual is the culmination of a three-year North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence initiative to draft a manual on the international law of cyber warfare. Because it was a NATO effort, none of the independent experts involved in drafting it were from Asia. Yet, absent other comprehensive efforts, the manual will likely increasingly be used as a reference in clarifying the state of play and rules of engagement in cyber space.

The silence of rising East Asian countries on this matter is deafening. It reflects poorly on changing international power dynamics and generates a dichotomy between the strategic environments in the real world and the virtual one. It also entrenches existing imbalances in power structures in the world and promotes a hierarchy of influence in the cyber domain, which in turn perpetuates trust deficits among major players. Worse, it is a damning indictment of the lag in thought leadership in East Asia on an increasingly significant issue. That the region's cyber space has been tested by mounting waves of attacks of varying severity points to the likelihood that these will escalate in magnitude and frequency in the future. How much longer will East Asia linger on the sidelines, prioritizing cyber space only within the confines of transnational crime and economic integration, before it decides to proactively shape evolving norms and rules? This is not to suggest the militarization of cyber space within or by East Asia. However, every country with critical infrastructure wired to cyber space has a stake in this unfolding conversation, and it is in the interest of each of them to ensure that cyber operations are conducted following a clear, just, and equitable set of rules accepted by most, if not all, states.

One encouraging development was the recent report of the UN Group of Government Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Comprising experts from Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the United Kingdom, and the United States, the GGE noted the applicability of international law, particularly the UN Charter and its importance "to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[25] It recommended confidence-building and capacity-building measures between and among states, but also with the cooperation of the private sector and civil society organizations, to build upon work being done by regional organizations and the United Nations.

ASEAN-Japan Cooperation in Strategic Cyber Security: The Way Forward

An important proviso underlies ASEAN-Japan cooperation in contributing to a more strategically secure, predictable, and stable environment in cyber space. Because cyber space cuts across geographical borders, whether virtually through data packets bouncing between servers in different countries or physically through undersea fiber optic cables, any strategic partnership in this area should be inclusive of the whole region. Cooperation between ASEAN and Japan should aim to temper the accusatory tenor that pervades present discussions on cyber security in the region. The idea should be to promote trust and build confidence rather than to utilize cyber space as another domain to chart strategic maneuvers for power and influence.

Mirroring much of ASEAN's approach to cyber security, ASEAN-Japan collaboration in this field has been similarly driven by the priority of securing the business environment.[26] Even the recent statement of the ASEAN-Japan ministerial policy meeting on cyber security cooperation explicitly puts a premium on this priority.[27] Five specific recommendations follow for ASEAN-Japan cooperation to bolster strategic cyber security going forward.

First, awareness of the matter, particularly within ASEAN, needs to be raised and cultivated. If security and defense mechanisms within ASEAN—including the ASEAN Regional Forum (ARF) and the ASEAN Defense

Ministers Meeting Plus (ADMM-Plus)—are to be taken seriously in a changing security environment, ASEAN and its partners must start considering cyber security beyond its currently narrow lens. Strategic cyber security draws on a collaboration of various other skill sets beyond just technical expertise, including diplomacy, politics, and the law. After all, cyber attacks against a state's CNII have geopolitical and legal implications and the technical solutions should be guided by an informed policy umbrella. This will require increased discussions and exchanges at the governmental (Track 1) and nongovernmental (Track 2) levels, both within ASEAN and between Japan and ASEAN, particularly among legal experts and senior policymakers. Awareness raising in this way will not necessarily divert resources away from ongoing cyber security initiatives, especially if discussions are conducted virtually on a sufficiently regular basis. ASEAN and Japan can lead and coordinate these efforts, but where relevant, other states in the region should also be included in these conversations to encourage transparency and goodwill.

Second, national cyber security strategies provide a good starting point in terms of putting policy into practice. Several ASEAN countries have their own strategies, and Japan recently drew up a new strategy to replace its older "Information Security Strategy for Protecting the Nation."[28] The details of these strategies are publicly available and can be easily shared among nations, so the added value in any further discussion related to these should be in giving special consideration to the role of the state in crafting rules of engagement for cyber operations, since the state is the primary arbiter of peace, security, and conflict, whether in the physical or virtual domain. Specifically, in considering each of these national cyber security strategies, ASEAN and Japan can determine whether they provide an adequate and relevant base from which to draw a regional approach regarding the applicability of international law to cyber space.

Third, policy and paper should be supplemented by preparation. At the Track 1 level, regional security cooperation could be expanded to include tabletop exercises and simulations in cyber space to improve responses to cyber attacks; advance clarity of action; and promote transparency, confidence, and trust among countries. These exercises could be held on the sidelines of ASEAN-Japan, ARF, or ADMM-Plus meetings, with other states invited to be observers if no objection is made to their full participation. The concept of interoperability in military affairs could be observed in the virtual realm so that decisions and actions are synchronized as best as possible in the event of a major cyber attack. With the infrastructure of cyber space stretching across borders, thereby raising the possibility of consequences spilling over to neighboring countries, and with ASEAN's impending integration, coordinated cooperation through exercises and simulations should increasingly be the norm.

Fourth, because of the multifaceted challenges that cyber space generates, a multipronged approach involving the private sector, Track 2 participants, and other relevant stakeholders must be taken to manage these risks. Although the private sector occupies the main part of contemporary discussions on cyber security because of the technical expertise residing within it, it is often not included in an integrated fashion in public policy efforts. The private sector's technical skills can be best leveraged when there is an understanding of policy directions. The two sectors, however, often speak past each other—that is when they are not speaking in entirely different languages altogether. This public/private dichotomy is especially ensconced in Southeast Asia, but it is less stark in Northeast Asia because of the closer defense and security relationship between the public and private sectors there. Accordingly, there are perhaps methods for including the private sector more comprehensively into policy discussions that ASEAN countries could learn from their Northeast Asian counterparts. For developing ASEAN countries with a nascent cyber security landscape, incorporating private-sector perspectives into government decisions would streamline and fast-track harmonization of public/private efforts from an early stage.

Drawing from the preceding recommendation, governments and the private sector could jointly organize simulations at information technology security conferences or policy roundtables around the region to create awareness of (1) the technical challenges of cyber security (which would benefit the public sector) and, conversely, (2) the overarching policies that guide cyber operations (which would benefit the private sector). These exercises would promote greater interaction and understanding between the public and private sectors.

Fifth, given the political sensitivities of cyber security in East Asia, there is a role for Track 2 institutions in East Asia—particularly ASEAN and Japanese think tanks—to take the lead in promoting strategic cyber security where Track 1 government-to-government forums are unable or unwilling to do so. Track 2 meetings offer three specific, related advantages. They are able (1) to draw representation from among diverse expert stakeholders, including the government, international lawyers, and regional and international organizations such as the ASEAN Secretariat, the International Committee of the Red Cross (ICRC), and relevant UN agencies and, by enabling these participants to exchange views in their personal capacities, facilitate discussions of even delicate matters; (2) to allow participants to speak in a frank and candid manner behind closed doors, if necessary, without concerns about attribution; and (3) to submit policy recommendations cognizant of, but unbound by, the political constraints that cloud government discussions. ASEAN and Japanese think tanks, in collaboration with thought leaders like the ICRC (which has already been considering strategic cyber security and its international legal implications) could initiate a series of policy roundtables specific to this purpose with the aim of proposing recommendations to national governments in the region.

Conclusion

ASEAN's drive toward economic integration and differences in its members' developmental and technological infrastructure presently supersede what is often viewed as a first world consideration. Strategic cyber security—as well as its manifestations of defensive and offensive capabilities, organizational structures, and policies—has been the preserve of the "haves" rather than the "have-nots." However, as less developed countries in East Asia are discovering, cyber space has the potential to be a great equalizer in the asymmetry of regional and international power.

Each and every country that is dependent on technology and the Internet—and this will only become more of a truism—is vulnerable to the security risks that cyber space presents, if not now, then certainly later. The rules for state behavior in cyber space and that of entities under their authority are an extension of the international legal framework governing relations between countries in the real world. The specifics of how the former differ from the latter, however, are still being debated.

A clear national position on these issues would clarify interactions and negotiations at the regional and global level. But a robust East Asian approach would ensure that the region's perspectives are well reflected and represented as international norms and laws crystallize. This is an opportunity for ASEAN and Japan to lead rather than defer or detract.

Notes

1. There are differing ways of spelling and defining cyber space—each with its own implications—observed by a number of countries and the International Telecommunications Union. For an overview of this, see Damir Rajnovic, "Cyberspace—What Is It?," *Cisco Blog–Security*, July 26, 2012, https://blogs.cisco.com/security/cyberspace-what-is-it/. The definition offered in this paper draws on the commonalities of these various definitions.
2. The ASEAN Broadband Corridor "aims to promote greater broadband penetration, affordability and universal access in ASEAN in order to enhance economic growth. It

aims to create an environment where e-business, e-commerce, venture capital, talents and ideas flow easily so that the region is better positioned to tap into the benefits of ICT and keep pace with the rapid development in other parts of the world." "Institutional Connectivity: ASEAN Broadband Corridor," Project Information Sheet MPAC PP/A3/01, in *ASEAN Connectivity: Project Information Sheets* (Jakarta: ASEAN Secretariat, 2012), 11.

3. In the early 2000s, "cyber" references in ASEAN communiqués and statements were driven by an agenda to counter transnational crime and terrorist use of the Internet. This was sparked in large part by the exposures in 2000 of the Jemaah Islamiyah network in Southeast Asia and the 2001 terrorist attacks in the United States. See, for example, the Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime, adopted by the 2nd Senior Officials Meeting on Transnational Crime, Kuala Lumpur, May 17, 2002, and the ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, Kuala Lumpur, July 28, 2006.

4. See, for example, the chapter on "Connectivity" in United Nations Economic and Social Commission for Asia and the Pacific, *Statistical Yearbook for Asia and the Pacific 2013*, http://www.unescap.org/stat/data/syb2013/H.1-ICT.asp; and *Southeast Asia Digital Future in Focus 2013: Key Insights and Digital Trends from Southeast Asia*, comScore, Inc., July 26. 2013.

5. See, for example, the Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime; the ASEAN Convention on Counter Terrorism, January 13, 2007; and Security Cooperation Division, ASEAN Political-Security Department, *ASEAN Documents on Combating Transnational Crime and Terrorism: A Compilation of ASEAN Declarations, Joint Declarations and Statements of Combating Transnational Crime and Terrorism* (Jakarta: ASEAN, 2012).

6. UN Conference on Trade and Development (UNCTAD), *Review of E-commerce Legislation Harmonization in the Association of Southeast Asian Nations* (Geneva: UNCTAD, 2013), http://unctad.org/en/PublicationsLibrary/dtlstict2013d1_en.pdf.

7. Ibid., 5.

8. James A. Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (New York: UN Institute for Disarmament and Research, 2013), 1.

9. Ibid., 2.

10 See, for example, the report released by US Transportation Department's inspector general that noted the multiple occasions on which civilian air traffic computer networks had been hacked into: Federal Aviation Administration, *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems* (FI-2009-049), May 4, 2009, http://www.oig.dot.gov/sites/dot/files/pdfdocs/ATC_Web_Report.pdf; and Siobhan Gorman, "FAA's Air-Traffic Networks Breached by Hackers," *Wall Street Journal*, May 7, 2009, http://online.wsj.com/news/articles/SB124165272826193727.

11. Gorman, "FAA's Air-Traffic Networks."

12. David Sanger, "Obama Order Sped Up Wave of Cyber Attacks against Iran," *New York Times*, June 1, 2012.

13. John Naughton, "US Fears Back-Door Routes into the Net because It's Building Them Too," *The Guardian*, October 13, 2013, http://www.theguardian.com/technology/2013/oct/13/us-scared-back-door-routes-computers-snowden-nsa.

14. Until 2012, Laos was the only ASEAN country without a national CERT/CIRT. LaoCERT has since been set up and is now an independent center under the purview

of the country's Ministry of Post and Telecommunications. See, website of the Lao Computer Emergency Response Team: https://www.laocert.gov.la/en/Page-1-.

15. Article 51 of the UN Charter states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

16. Google Malaysia's website, for example, was hacked by a Pakistani group called "TeaM MADLEETS." See, Fahirul Ramli, "Google Malaysia Search Engine Page Hacked," *New Straits Times*, October 11, 2013. At the height of the Lahad Datu incursion in Sabah by a group of Sulu insurgents, websites in the Philippines and Malaysia were hacked by sympathizers of both sides of the conflict. See, "Sabah Row Spills Over Online: PHL, MY Sites Defaced," GMA News Online, March 3, 2013, http://www.gmanetwork.com/news/story/297507/scitech/technology/sabah-row-spills-over-online-phl-my-sites-defaced. The Singaporean prime minister's and president's websites were also hacked in early November 2013 by individuals believed to be linked to "Anonymous." See Andrea Tan, "Singapore Probes Five, Charges Another over Web Hacking," *Bloomberg.com*, November 12, 2013, http://www.bloomberg.com/news/2013-11-12/man-in-singapore-charged-with-defacing-website-after-cyberattack.html.

17. "'Anonymous' Attacks Websites in Neighbouring Countries, Says Report," *Malaysian Insider*, November 4, 2013, http://www.themalaysianinsider.com/malaysia/article/anonymous-attacks-websites-in-neighbouring-countries-says-report.

18. In 2011, Japan's Mitsubishi Heavy Industries was reportedly the subject of a cyber attack targeting data on missiles, submarines, and nuclear power plants. See "Japan Defence Firm Mitsubishi Heavy in Cyber Attack," *BBC News*, September 20, 2011, http://www.bbc.co.uk/news/world-asia-pacific-14982906. South Korea sustained economic losses amounting to 800 billion won (nearly US$8 million) in the latest wave of cyber attacks from March to June 2013, which affected the president's website, three television stations, six banks, and 30,000 computers. See Alex Hern, "North Korean 'Cyberwarfare' Said to Have Cost South Korea £500m," *Guardian*, October 16, 2013, http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea.

19. "South Korea Accuses North of Cyber Attacks," Reuters, July 16, 2013, http://www.reuters.com/article/2013/07/16/net-us-korea-cyber-idUSBRE96F0A920130716; "Four Years of DarkSeoul Cyberattacks against South Korea Continue on Anniversary of Korean War," Symantec Official Blog, June 26, 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.

20. Article 2(4) of the UN Charter states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

21. The International Court of Justice has noted that no definition of an "armed attack" is available in the UN Charter or in treaty law. *Case Concerning the Military and Paramilitary*

Activities in and against Nicaragua (Nicaragua v. United States of America), June 27, 1986, International Court of Justice Reports 1986, notes 64, 94, para. 176.

22. For a more detailed discussion, see Marco Roscini, “World Wide Warfare—Jus Ad Bellum and the Use of Cyber Force,” in *Max Planck Yearbook of United Nations Law Vol. 14*, ed. Armin von Bogdandy and Rüdiger Wolfrum (Netherlands: Brill, 2010), 85–130.
23. See, for example, Daniel Rosenfield, “Rethinking Cyber War,” *Critical Review: A Journal of Politics and Society* 21, no. 1 (2009): 77–90; and Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.
24. Harold Hongju Koh, “International Law in Cyberspace” (remarks presented at USCYBERCOM Inter-Agency Legal Conference, Maryland, September 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.
25. United Nations General Assembly, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)” (June 24, 2013), para. 19.
26. For a description of ASEAN-Japan meetings and workshops on information security since 2009, see “ASEAN-Japan Collaboration on Information Security,” National Information Security Center, Japan, http://www.nisc.go.jp/eng/fw_top.html.
27. “Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation,” Tokyo, September 13, 2013. The statement pledges to promote ASEAN-Japan efforts to create a secure business environment, build a secure information and communication network through technical cooperation, and enhance capacity for cyber security including critical infrastructure protection and business continuity plans for ICT.
28. “Cyber Security Strategy,” Information Security Policy Council, Japan, June 10, 2013, http://www.nisc.go.jp/eng/pdf/CyberSecurityStrategy.pdf.