CSCAP Cybersecurity Workshop
Conference Report
April 5, 2017 Semarang, Indonesia
Final

While information and communications technology continues to provide immense opportunities and benefits for economic and social development, cybersecurity is assuming an increasingly high-profile role in the Asia-Pacific security calculus. This reflects the deepening penetration of information and communications technologies into the daily life of regional governments, businesses, and citizens, and an expanding array of threats as a result of that evolution. Dangers include: criminal acts (data theft or modification or ransomware attacks); strategic attacks (on critical infrastructure or other key cyber systems); misuse of the Internet for terrorist purposes (as a platform for recruitment, financing, and radicalization); and cyber-enabled interference with electoral processes. At the 19th ASEAN Regional Forum (ARF) Ministerial Meeting in July 2012, ARF foreign ministers adopted a Statement of Cooperation on Ensuring Cybersecurity; two years later, at the 21st ARF Ministerial Meeting, the chair tasked officials to develop a work plan that addressed practical cooperation and confidence building measures. In the following year, at the 22nd ARF Ministerial Meeting, attendees adopted the ARF Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs Security). Singapore held the inaugural ASEAN Ministerial Conference on Cybersecurity (AMCC) on Oct. 11, 2016, at which Singapore's SG$10 million ASEAN Cyber Capacity Program was launched. The momentum to develop practical cooperation and cyber confidence-building measures has slowed, however, and while concern in the Asia-Pacific region about cyber threats has grown and intensified, concrete measures to address and counter those challenges have been slow to materialize. Discussions have continued and there has been a growing chorus of frustration about the lack of progress to implement the measures identified in the work plan.

In an attempt to prod that process, the US and Indonesia member committees of the Council for Security Cooperation in the Asia Pacific (USCSCAP and CSCAP Indonesia, respectively) co-hosted on April 5, 2017 a one-day workshop on cybersecurity in Semarang, Indonesia. We convened the day before an ARF Inter-sessional Meeting on Counter-terrorism and Transnational Crime that examined cyber issues, among others. Thirty officials and experts from 15 countries, economies, and institutions, all attending in their private capacity, discussed the regional cybersecurity environment, progress that has been made in ASEAN since articulation of the ASEAN Cybersecurity Cooperation Strategy, and confidence-building measures that can help the ARF achieve a safer regional cybersecurity environment. The report that follows summarizes those discussions; it reflects the views of the chair and is not a consensus document.

The Asia-Pacific cybersecurity environment

Cyber threats pose an increasingly serious challenge to regional security. One study estimates cyber crime resulted in $81 billion in damage to the Asia Pacific during the 12-month period ending in September 2015, an amount that exceeds by $20 billion the costs of cyber crime in North America and the EU. More worrisome still, the number of such incidents is growing. Governments are also troubled by the threat of online radicalization and other content-related issues. In addition,

there is growing recognition that information and communications technology (ICT) networks and servers themselves, including those that support critical infrastructure, are vulnerable to malicious cyber activities. In many ways, ASEAN's future growth and prosperity are threatened by proliferating cyber threats.

In her presentation, Mihoko Matsubara (*Palo Alto Networks*) analyzed the forces driving cyber crime, highlighting the role of basic economics. Research revealed that 60 percent of adversaries are driven by profit and 72 percent are opportunistic. In other words, the vast majority of such incidents are motivated by the desire for "an easy score" and "bad guys" are not conducting long campaigns. The conclusion to be drawn is that increasing the costs associated with conducting cyber crime can significantly change adversaries' behavior; 69 percent would quit and move on to a new target if defenses are strong. Similarly, nearly 40 percent of attacks can be prevented by sharing information, a finding that underscores a fundamental truth about cybersecurity: cooperation is critical to defeating these threats. To put this in real terms: hackers often use off-the-shelf tools (programs and exploits) to carry out cyber crime. When hacked organizations share information about their vulnerabilities (and use that information to shore up their defenses), hackers are forced to customize those tools, which increases their costs.

Fortunately, there is growing awareness of those threats among the government and private sectors. As Elina Noor (*Institute of Strategic and International Studies (ISIS) Malaysia*) noted, regional governments are paying more attention to cyber issues and are especially worried about online radicalization; 70 percent of detainees arrested for extremism in Malaysia in 2015 were radicalized online through social media. For Southeast Asian countries where there are competing views of the national narrative, cyberspace is an especially contested domain – a cyber threat that is relatively unappreciated by non-Southeast Asian observers, suggested Noor. Cybersecurity is a regular agenda item in a variety of national and international forums. In Asia, CSCAP drafted a Memorandum on Cybersecurity, which it presented to the ARF in 2012. The 2015 ARF Work Plan on Security of and in the Use of Information and Communications Technologies and the 2016 AMCC are important milestones in regional efforts to tackle these problems.

Unfortunately, there is also consensus that more must be urgently done and a more robust policy is needed at the national and regional levels. The ARF Work Plan put forward many recommendations but, despite this consensus, implementation has been limited. In addition to enhanced government-to-government engagement, dialogue among all stakeholders should be strengthened. There must be conversations between business and governments, and the technical community as well. Noor underscored that states must address cybersecurity at a strategic level, as well as from a holistic perspective that includes all key constituencies.

Discussion highlighted and developed several points made during presentations.

First, the assembled experts agreed that all stakeholders must be engaged. Governments can set policies, but must take into account that the private sector is usually the target of cyber attacks and it must build defenses against hackers. Companies should acknowledge when they have been attacked and defenses breached – which can be difficult. Reputational damage can be severe and companies are loath to expose vulnerabilities to competitors. The technical community must be involved since it is responsible for devising defenses. Civil society should be included to ensure

that individual interests are represented as well. But while discussions should be as inclusive as possible, the more constituencies that are represented, the more difficult it will be to agree on priorities and responses. Some participants pointed to the lack of communication among different agencies and ministries addressing these problems and a divergence of priorities among them. Still, they also noted a growing awareness of the need to acknowledge vulnerabilities, especially in the business sector.

Second, there is an extensive body of work that can be used to articulate a framework of responsible state behavior in cyberspace and improve cyber incident responses, at the governmental and institutional levels. This is especially evident in the case of confidence building measures (CBMs), which are taken up in more detail in session three. In other words, there is no need to start from scratch as ASEAN and the ARF address cyber threats. There are also a number of forums holding conversations about cybersecurity. At the same time, participants acknowledged the need to draw upon – rather than adopt without comment – initiatives that work. Solutions must be tailored to regional circumstances. For example, in addition to different approaches to cyber CBMs, there are institutional differences: the OSCE has extensive secretariat support while the ARF processes are more member driven.

A third key point was the need for a common lexicon or vocabulary to discuss cyber issues. The rhetoric of cybersecurity changes depending on who is talking and what is being discussed. So, for example, technology specialists called for differentiation between "cyber threats" and "cyber enabled threats," while policy-makers explored distinctions regarding various meanings of the word "attack." Meanwhile, an academic pondered the meaning of "strategic cybersecurity," wondering if our group could find consensus on the term. This discussion led to consideration of a lexicon or sharing of definitions of cyber terms, a process that would not necessarily forge agreement on a single usage and vocabulary but would be intended to improve regional understanding. This could lead to a comparative study of approaches to threats as viewed across the region, which could yield a better sense of shared priorities – and, perhaps more important, divergences.

Progress in ASEAN

Cybersecurity has assumed an increasingly prominent profile in Asia-Pacific institutions and meetings. In 2012, the ARF adopted the Statement on Cooperation in Ensuring Cybersecurity. Two years later, the ARF was tasked with drawing up a work plan, an assignment that was completed by May 2015. A series of workshops and seminars followed: a July 2015 workshop on Cybersecurity Capacity Building; an October 2015 seminar on Operationalizing Confidence Building Measures in the ARF; and a March 2016 workshop on Operationalizing Confidence-Building Measures for Cooperation During Cyber Incidents. The 2016 AMCC signaled the organization's concern about cyber threats and its readiness to take up that challenge in that institutionalized way.

Joe Burton (*University of Waikato*) applauded this evolution, in particular ASEAN's readiness to develop a cybersecurity cooperation strategy that is based on the centrality of information technology and communications security to ASEAN's growth and future prosperity. Burton argued that ASEAN, with its distinctive form of cooperation, could be a world leader and a model

for regions as they pursue cybersecurity. He pointed to the region's focus on capacity building, which is always relevant but is even more critical when a region is establishing its cyber infrastructure. This allows planners to "build security in" rather than "add it to" existing capacity.

A second ASEAN advantage is its focus on confidence building and the promotion of measures to stimulate transparency, trust, and dialogue. These efforts build on existing levels of trust and confidence; the organization is not starting from scratch. While those projects are occurring both among ASEAN members and with outside actors, the emphasis is on internal processes. Burton highlighted ASEAN's approach, one that recognizes and adapts to the organization's political diversity as well as to the region's norms.

Wei Kee Tan (*Cyber Security Agency of Singapore*) explained how his country is addressing cybersecurity and its work for ASEAN. He too emphasized ASEAN's proactive cyber strategy, an outlook built upon the realization that cyberspace is the enabler of economic progress and the improvement of living standards. He identified the October 2016 AMCC as useful in establishing a platform for discussion of cyber issues among both ICT and cybersecurity ministers and senior officials and harmonizing perspectives. There, ASEAN representatives agreed on a Cybersecurity Cooperation Strategy that set out a road map that focused on the importance of strong and coordinated cooperation in areas such as cybersecurity policy, strategy development, legislation, norms and capacity building. In this regard, at the 16th TELMIN in November 2016 and at the TELSOM-ATRC Leaders Retreat in March 2017, the ASEAN Cybersecurity Cooperation Strategy was endorsed and approved, setting out a road map that focused on three areas: incident response; policy building and coordination among Computer Emergency Readiness Teams (CERT); and cybersecurity capacity building. To that end, the strategy, which Singapore drafted in its capacity as Vice Chair of the ASEAN Network Security Action Council (ANSAC), with input from ASEAN member states, includes an ASEAN CERT Maturity framework, a self-assessment tool to help each ASEAN state analyze its national CERT's maturity, identify areas to improve, and assess the progress made. Inputs from each member country will help ANSAC establish a list of action areas for coordinated cybersecurity cooperation and training. In addition, ASEAN is monitoring the suitability of initiatives undertaken elsewhere to facilitate progress. Tan explained that, as a follow-up, Singapore will be holding "train the trainer" workshops to familiarize ASEAN member states with the CERT Maturity Framework so as to maximize impact and effectiveness.

One of the projects under Initiative 8.2 on strengthening information security preparedness in the ASEAN ICT Masterplan 2020 (AIM2020) is a feasibility study on establishing an ASEAN CERT. An ASEAN CERT could be set up as a formal mechanism through which national CERTs in ASEAN can coordinate and collaborate to boost regional effectiveness in incident response. The feasibility study will be implemented in 2018.

A first step in this process is the establishment by Singapore of an SG$10 million ASEAN Cyber Capacity Programme to develop a suite of modular, flexible, and multi-disciplinary initiatives to help build ASEAN cybersecurity capacity across technical and policy areas. These initiatives will take a multinational, multi-stakeholder approach that includes all important constituencies. The process began with a workshop on cyber norms that was held in May 2017 to raise awareness and initiate discussions among ASEAN. This workshop is anticipated to be the first of several.

Andi Widjajanto (*Indonesia National Task Force of the Cybersecurity Agency*) explained that Indonesia doesn't have a cybersecurity architecture per se. There is a law concerning internet transactions but there is no national policy or single institution that addresses the issue. Authorities are dispersed, expertise is limited, and digital infrastructure is being developed. The Cybersecurity Agency will not be officially launched until May 2017.

Still, Jakarta recognizes its deficiencies and has ambitions: it aims to reach Singapore's cyber capability by 2020. To do so, it is utilizing the "collaborative networking model" that Europe has embraced, using advanced technology, a purely defensive cyber doctrine, and a multi-stakeholder approach. Widjajanto distinguished between an approach that focused on cybersecurity and one that sought to build "Digital Indonesia," noting that his government adopted the latter. To that end, emphasis is on collaborative networking, rather than state sovereignty or standardization.

Europe is ready to help. The EU is stepping up work on cyber capacity building in third countries, in particular to strengthen technical and organizational cyber incident response capacity in partner countries. This effort is an integral part of the EU external action plan on cybersecurity (as articulated in the 2013 EU Cybersecurity Strategy), which is in turn linked to the EU development agenda. Central to this program is the Budapest Convention on Cybercrime, which establishes a framework for international cooperation. Europe plans to do still more via the "Instrument contributing to Stability and Peace" (IcSP), which is slated to include an 11 million euro action plan, "Capacity Building and Cooperation to Enhance Cyber Resilience," that is scheduled to commence this year.

Again, discussion underscored the need for a better understanding of the regional cybersecurity status quo. Effective capacity building demands first an accurate assessment of the capacity of target states and second, realistic appraisals of potential progress. It is not clear that ASEAN as an institution and member states individually can make those judgments. The second inquiry will yield an understanding of the lessons ASEAN has learned during implementation of its cyber strategy. What are the chief obstacles to progress, and what is holding up implementation of CBMs already recommended in the 2015 work plan? Is it political will or institutional and technical capacity? One ASEAN member state representative bemoaned the organization's lack of progress on CBMs generally, and not just those related to cybersecurity. Progress ultimately depends on shared priorities, a shared vocabulary, a multi-stakeholder approach, and a readiness to tailor solutions to the particular needs of individual states. One ASEAN member observed that cooperation may be easier among countries with ***fewer*** overlapping geopolitical interests, a comment that has profound implications: if the prospects for effective cyber partnerships are inversely related to geopolitical convergence, then the rhetoric of cooperation masks a lack of trust among Asia-Pacific states.

For all the challenges, there was consensus that ASEAN could be a model for regional cybersecurity cooperation. As participants surveyed venues for engagement on cybersecurity, there was also agreement that the ARF is the best Asian regional security venue for such efforts.

Confidence Building Measures

There is no shortage of ideas on how to build confidence among states in cyberspace. As Klee Aiken (*Asia Pacific Network Information Center, APNIC*) pointed out, ASEAN has already identified and incorporated best practices in the 11 work areas of its work plan. He warned that since the last scheduled meeting of the work plan has been held, the working agenda should be renewed. He called for more meetings to make habitual regular contact and interaction among stakeholders; he would like to see more conversations among policy and technical groups to bridge the gap that exists between them regarding understanding of the issues and problem solving. He called for "small meaningful progress with quick wins," championing the creation of the Point of Contacts list, discussions, and tabletop exercises. As always, a shared understanding of what is and isn't happening is critical, as well as agreement on the reasons for progress – or the lack thereof.

Sheila Flynn (*Office of the Cyber Coordinator, US Department of State*) highlighted the importance of CBMs, noting that the difficulty of attributing the origins of behavior in cyberspace puts a premium on trust. The value of this premium is magnified since the effects of malicious cyber incidents can ripple far beyond national boundaries and intended targets. Effective prevention, mitigation, and response measures demand working relationships among governments and other key players, and that is only possible if there is trust among them. A key element in the trust and confidence building process is knowing who critical interlocutors are when there are crises or emergencies: that is why points of contact lists are so important. Without that list, embassies become critical in figuring out who to talk to about cyber issues in host countries, and communication channels can be limited to established contacts – not necessarily the best or the right interlocutors. Flynn, like others, singled out the ARF as the best venue for regional cybersecurity discussions, praising the work it has done, while urging it to do more.

Cooperation is most effective when all parties have an accurate assessment of their own cyber maturity and that of their collaborators. Thus, Zoe Hawkins (*Australian Strategic Policy Institute*) highlighted the need to establish awareness of the state of national cybersecurity programs and the setting of meaningful baselines – read: expectations – for partners. Her organization has endeavored to do so through its report *Cyber Maturity in the Asia Pacific*. This annual analysis utilizes public information to create national cyber policy profiles that can be used to inform international cooperation. Hawkins noted that the very process of compiling such reports helps create situational awareness of national roles and responsibilities for cyber policy, and that if conducted collectively at an official level within the ARF could help build transparency between countries. Like other speakers, she noted that a key part of this effort is detailing points of contact across a range of national agencies and interests. She also warned against the creation of "capacity darlings," countries that absorb disproportionate amounts of foreign assistance: while they provide successful examples of capacity building, they may not be the most efficient use of limited resources.

Maria Smekalova (*Russian International Affairs Council*) reiterated the call for more information about the cyber status quo and the desirability of small steps to build trust, promote cooperation, and build momentum for more meaningful collaboration. She warned against overly ambitious agendas, given not only the fitful progress to date, but also the speed with which bad actors adapt

to a changing environment. She recommended a focus on critical infrastructure, such as civil nuclear energy facilities and financial institutions, and applauded the bilateral Russia-US projects that seek to promote information sharing, which is hoped will lead to information exchanges and the expectation of reciprocity. Streamlining of cyber information exchanges should be a priority; she suggested that Interpol could be the best international platform to fight cyber crime.

For those who worry about the Asia-Pacific region's progress in combatting cyber threats, Stefan Soesanto (*European Council on Foreign Relations*) provided a useful reality check by explaining Europe's actions in this area. While the Organization for Security Cooperation in Europe (OSCE) has adopted two sets of regional CBMS – 11 in December 2013 and 5 in February 2016 – Soesanto bemoaned the lack of progress in implementing them. Ninety percent of OSCE members have implemented just one or more, a figure that is less impressive on inspection than first glance. The University of Florence is creating a matrix of implementation; preliminary results from that effort were reported at the OSCE November 2016 workshop on attribution, an event that sought to draw conclusions on the scope for building "impartial" verification into OSCE work on cyber CBMs. He questioned whether the OSCE is getting the right people in the conversation. The current emphasis seems to be on foreign and defense ministries; he wondered whether it would be more productive to include intelligence and law enforcement agencies, suggesting their involvement could reduce tensions and miscalculations.

According to Soesanto, EU efforts to promote cyber cooperation are built on four pillars: a NIS (Network Information Security) directive, which (loosely) defines critical infrastructure (CI), designates authorities for CI contacts and introduces mandatory reporting requirements for CI; the general data protection regulation, which imposes mandatory reporting requirements on businesses and organizations to notify the national supervisory authority when they have been hacked; the European Investigative Order, which accelerates the mutual legal assistance process by harmonizing request forms and sets time limits on responses; and a cyber-diplomacy toolbox, that will "include instruments that are suitable both for immediate response to incidents as well as elements that can be used to punish or deter coercive cyber operations in the longer term." More information on that toolbox is not yet available. Soesanto also applauded the EU's Joint Cybercrime Action Taskforce (J-CAT), which includes cyber liaison officers from some EU member states, several non-EU law enforcement partners, and the Europol Cybercrime Center.

Other participants expanded on Europe's efforts to share its experience with CBMs. The EU made presentations on its CBM work at a March 2014 ARF workshop, and the EU and OSCE organized a cybersecurity workshop with the ARF in March 2016.

The most important CBM appears to be regular and trusted channels of communication. Cybersecurity constituencies – policy makers, business interests, government security institutions and agencies, and technical specialists – need to know their counterparts in other governments and organizations, trust them, and have confidence that when they reach out, they will be answered in a timely and meaningful way. As our discussion makes clear, a meaningful and productive dialogue requires common understanding of: interlocutors' standing and interests (to ensure that the right people are talking to each other); words and vocabulary (so that there is better understanding of what one's words/vocabulary mean); and venues for engagement (a particular platform is the appropriate place to have a particular conversation).

Central to progress is standardization of expectations, formats, and procedures. Baselines are needed so that countries can assess their standing and capabilities relative to others and so that partners will have realistic expectations of them. Templates can be established that address how to share information, how to request assistance, and how to pursue legal action. Points of contact lists will identify who to talk to about particular problems.

Participants identified several ways that CSCAP could assist in this endeavor. It could provide comparative research on threat perceptions among its member committees. It could provide a venue for standardized presentations on national capabilities. It could conduct research on regional approaches to CBMs (something it has already done for the ARF on the topic of Preventive Diplomacy). CSCAP's involvement could also address the thorny issue of ensuring that Asia-Pacific solutions reflect particular concerns of Asia-Pacific countries. The group agreed that a valuable first step for any CBM project within the ARF would be inauguration of the ARF ICT Security ISM and/or ARF Study Group on Confidence Building Measures and compilation of the ARF Directory of Cyber Points of Contact.

It was also recommended that:

- ARF member governments develop and share national cyber strategies that reflect whole-of-government roles and responsibilities.
- ARF member governments compile and compare national assessments of cyber threats, their consequences, and the priority they assign those threats.
- stakeholders aggressively promote the idea that cybersecurity promotes confidence and facilitates economic growth and development.
- stakeholders share lists of key cyber terms to improve regional communication.
- stakeholders utilize maturity frameworks or other best-practices models to assess national status of and progress in the implementation of cybersecurity policies. Establishing a more robust baseline of the status of national cybersecurity efforts is imperative.
- countries and organizations offering assistance in capacity building coordinate to minimize duplication. Donor countries could develop a template that identifies the assistance they can provide and maintain them in a single repository. At the same time, such efforts must be tailored to recipients; there is no "one size fits all" formula for capacity building. A standard template for assistance could also be developed and maintained with the assistance offers.
- meetings of regional cybersecurity stakeholders be regular and routinized to promote habits of dialogue, information sharing, and cooperation.
- ARF member governments support ongoing cooperative cyber efforts in specific sectors, including mutual legal assistance and CERT cooperation.
- study the possibility of cross-regional engagements on cybersecurity, such as OSCE-ARF.

There are many reasons to be optimistic about the prospects for regional cybersecurity cooperation in the Asia Pacific. There is a broad consensus on the urgency of the problem and the need for collective action. Regional economic and security forums have acknowledged the desirability of addressing these concerns in a sustained and focused way. There are many ideas that offer constructive ways to combat regional cybersecurity challenges. And finally, preliminary steps have been taken in pursuit of these goals.

Unfortunately, there appears to be a disconnect between the urgency of the problems and the speed with which regional governments, individually and as a group, are effectively implementing measures that can tackle these challenges. In short, implementation is lagging. The most pressing task then for the ARF and its member states is finding the political will to close this gap.

This report was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the author[s] and do not necessarily reflect those of the United States Department of State.