NORMS FOR CYBERSECURITY IN SOUTHEAST ASIA

Policy Options for Collaborative Security in the Southeast Asian Region

CONTENTS

EXECUTIVE SUMMARY

Broad adoption of cybersecurity norms can help promote social and economic development, as well as improve the international security context in the Southeast Asian region by lending to the region's stability and creating a solid footing for further harmonization of policies. This paper outlines the existing efforts around cybersecurity norms and related activities in a variety of forums, and charts their development processes. It explains the benefits of collaborative cybersecurity for the region, and suggests some areas for the region's stakeholders to continue work on norms development:

- Establishing a common language to guide cybersecurity discussions.
- Developing policies for coordinated and responsible vulnerability disclosure.
- Encouraging cooperative information exchange to promote regional security.
- Building capacity within the region.
- Enshrining the multistakeholder model at the heart of the norm development processes.

NORMS: CONSENSUS DRIVEN PRINCIPLES FOR INTERNATIONAL CYBERSECURITY

Norms – defined as principles or standards of behavior expected of a member of a group – have a long-standing history in reducing conflict between states. More recently, norms have been discussed and developed as a means of reducing conflict in cyberspace, including the recommendation of a set of norms for responsible state behavior in cyberspace by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) in 2015.

The concept of norms has been transposed to cyberspace from other areas where international cooperation was needed. International norms have been developed in areas such as nuclear nonproliferation and human rights with great success in generation global consensus around key issues. Norms are different from binding international law or domestic regulation, in that deviation from them isn't unlawful, but may lead to censure by other actors. Norms can promote responsible behavior by actors in an international environment, thereby ensuring predictability and reinforcing stability. While only one of several tools for promoting international stability, they are generally easier to agree to than a treaty, and easier to change, making them adaptive to an ever-evolving international stage.

[1] Note by the Secretary-General on the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 24 June 2013. Available at: https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/%24FILE/A%2068%2098.pdf

[2] Consensus Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July 2015. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[3] NATO Cooperative Cyber Defense Centre of Excellence: "2015 UNGGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law" 31 August 2015. Available at: https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

Building upon the affirmation that international law is "applicable and essential to maintaining peace and stability and promoting an open secure, peaceful and accessible ICT environment[1]," cybersecurity norms are emerging in a variety of forums, including most prominently, the UNGGE The latter recommended a list of norms for responsible state behavior in cyberspace in 2015.[2] Even though the UNGGE negotiations included only a small group of countries and did not involve stakeholders from the private sector or civil society, the agreement reached in the 2015 Report represents an important step: Its adoption by the UN General Assembly marks the first global embrace of cybersecurity norms.

The 2015 UNGGE Report outlined 11 norms for responsible state behavior in cyberspace. These broad statements were agreed upon by the international community, although work remains to contextualize these and integrate them to national and international strategies. They can be grouped into two categories[3]: 1) norms that limit what states should do in cyberspace, and 2) those that speak to the duties of states in cyberspace. Briefly, the 2015 UNGGE norms were:

1. LIMITING NORMS

- **a.** States should not knowingly allow their territory to be used for wrongful acts using ICT.
- **b.** States should not support or conduct cyber-attacks that damage critical infrastructure.
- **c.** States should seek supply chain security and avoid proliferation of harmful tools and techniques into the market.
- **d.** States should consider all relevant information, when attributing cybersecurity incidents;
- **e.** States should avoid attacking Computer Emergency Response Teams (CERTs) and should not use CERTs for cyber-attacks.
- **f.** States should respect human rights online.

2. POSITIVE DUTIES OF STATES

- **a.** States should improve information sharing, in particular on terrorist and criminal use of ICTs.
- **b.** States should cooperate and respond to requests for assistance related to protecting their critical infrastructure.
- **c.** States should protect their critical infrastructure.
- **d.** States should engage in responsible reporting of ICT vulnerabilities.
- **e.** States should cooperate in developing and applying measures to increase stability and security in the use of ICTs.

The UNGGE process continued in 2017, with a goal of clarifying how the 2015 agreement should be implemented, but its members were unable to reach a consensus. Despite this setback, norms remain as, if not more, relevant and necessary today. As more countries, organizations, and people come online, a clear understanding of how they should interact in the complex cybersecurity environment is needed. The political setback at the UNGGE should therefore not stop work in this area.

Meanwhile, there are important opportunities for regional groupings to advance discussions on effective implementation of 2015 UNGGE norms, as well as to refine and contextualize them. Even if the global processes on the development of norms have stalled, smaller initiatives can still make progress and lead the global community to greater stability in cyberspace.

[4] OSCE, Decision No. 1202, 10 March 2016.
Available at: https://www.osce.org/pc/227281?download=true

Some work is already being done at the regional level such as the development of Confidence Building Measures (CBMs) by the Organization for Security Co-operation in Europe (OSCE) and the Association of Southeast Asian Nations (ASEAN). These CBMS aim to reduce the risk of cyber conflict between states. The CBMs include, inter alia, the sharing of best practices, law enforcement cooperation, and building a consensus glossary of terminology related to cybersecurity issues.[4]

Southeast Asia in particular stands to benefit from adoption and contextualization of cybersecurity norms. This is a region that is rapidly coming online, promising to become an innovation powerhouse for the future. At the same time, countries in this region are already experiencing intense cybersecurity threats, stemming from both rapid technology adoption which has led to a greater available attack surface for adversaries, and long-standing geopolitical pressures. Regional collaboration on developing cybersecurity norms can help build cyber resilience, as well as common understanding and trust. While initial work in this area has begun, in particular through bilateral conversations, more can and needs to be done to ensure the region can take its rightful place as a leader of global innovation.

CYBERSECURITY POLICY ACROSS SOUTH EAST ASIA

Cybersecurity challenges affect everyone, irrespective of nationality, sector or size. They cross borders, and evolve quickly. The impacts of cybersecurity incidents are felt worldwide, in both private and public sectors. As a result, any attempt to address them requires collaboration among and between appropriate stakeholders across the private and public sectors, and the flexibility to learn, adapt, and evolve as quickly as the attackers do. While there is no such thing as a perfect system or total security, collaboration between stakeholders can improve systems and increase the resiliency of increasingly important ICT networks.

Southeast Asia region is no exception. As a region it faces a very daunting and specific set of cybersecurity challenges.[5] These are the result of a very rapid adoption of technology and expansion of broadband access, coupled with regional and international geopolitical challenges translating into a new environment. Moreover, the countries in the region are at different stages of economic development, policy maturity, and technology adoption, meaning that the development of policy that meets the needs of all members must be considered carefully.

[5] Inquirer. Lucas, Daxim L: "More Southeast Asian Firms Vulnerable to Cyber Threats"2 October 2017 Available at: http://technology.inquirer.net/67509/southeast-asia-cyber-threats-on-rise-kaspersky-lab

However, despite those differences, countries in the region will be better placed addressing cybersecurity together than on their own. That does mean that the policies developed need to be focused on protecting the region's burgeoning infrastructure in its least developed countries, as well as protecting more complex digital societies and economies. It also means that an initiative, such as one focused on cybersecurity capacity building and cybersecurity norms would be especially helpful, as it would support the development of understanding of different countries positions and objectives.

Harmonization of policies and practices within the region and the broader Asia-Pacific context is already being undertaken, and promises to help bridge the region's digital divides. On privacy, for example, the APEC Cross Border Privacy Rules (CBPR) are a valuable feature of the region's economic integration and can also be used to promote cybersecurity. By adopting and promoting the CBPRs within the region, member states help guarantee the economic benefits of cross border data flows and cloud computing while ensuring that their citizens' data is always appropriately handled. Harmonized cybersecurity policies can have similar effects, enabling smaller markets to achieve benefits of scale by grouping together. Norms can help drive the development of sound domestic policy as well. A range of policy options can meet the objectives set forth in international norms, from strict compliance driven approaches to voluntary guidelines. In turn these policies can then reconfirm a country's commitment to adhering to a set of international principles, further building a truly global approach.

For example, governments that create an enabling environment for innovation tend to focus on the following cybersecurity policy outcomes:

- Permit organizations to respond to their threat environment in a risk-based, flexible, and dynamic way, even when legislation and regulation can't adapt quickly to new threats and mitigation techniques.
- Adopt a risk management framework that helps them to prioritize, risk, threat, and infrastructure they want to protect
- Build capacity within government and industry to identify, protect, detect, respond, and recover from attacks.
- Incentivize voluntary threat information sharing practices (including from government to industry) that build trust among organizations.
- Avoid blaming the victims of cyber-attacks, and instead protect them from adversarial regulatory reactions when they come forward about data breaches or other attacks.
- Contribute to the security of all users by sharing discovered vulnerabilities with industry actors in a timely fashion.

[6] Cyber Security Agency of Singapore, 17 September 2017. "ASEAN Member States Affirm Importance of Closer Coordination of Cybersecurity Efforts In ASEAN." Available at: https://www.csa.gov.sg/news/press-releases/amcc-2017

[7] www.first.org

[8] Nandikotkur, Geetha. Information Security Media Group, 31 January 2017: "New APAC Center to Coordinate Threat Info Sharing" Available at: https://www.bankinfosecurity.com/new-apac-center-to-coordinate-threat-info-sharing-a-9660

The region has already begun collaborating on cybersecurity. These efforts include the finalization in March 2017 of the ASEAN Cybersecurity Cooperation Strategy, which will provide a roadmap towards a more coordinated approach to building capacity in the area of incident response; the establishment of a new Inter-Sessional Meeting on Security of and in the use of ICTs under the ASEAN Regional Forum (ARF) platform to discuss issues such as confidence building measures; and the annual Cyber SEA Games to uncover and develop the next generation of cybersecurity talent and expertise. In addition, ASEAN Leaders and Ministers have affirmed at the recent 31st ASEAN Summit and the second ASEAN Ministerial Conference on Cybersecurity the need for closer coordination of cybersecurity efforts across the various ASEAN platforms as well as for moving discussions forward on the adoption of basic voluntary norms of behavior to guide responsible behaviour in the use of ICTs, taking reference from the recommendations in the 2015 UNGGE report[6]. Moreover, an increase in technical collaboration has led to greater sharing of information, and quicker and more effective responses to online threats. This has been done through global mechanisms, such as the Forum of Incident Response and Security Teams (FIRST)[7], as well as regional and bilateral working arrangements. Some countries in the region have also begun building information-sharing relationships with governments and industry stakeholder groups from outside the region, such as the Monetary Authority of Singapore's information-sharing relationship with the global Financial Services Information Sharing and Analysis Center (FS-ISAC)8.

MULTISTAKEHOLDER NORM DEVELOPMENT

Cybersecurity norms do not apply only to governments, in particular as much of the online infrastructure and cybersecurity expertise rests with the private sector. At the same time, cybersecurity frequently requires a national or broader discussion on balancing security with other rights. Therefore, for norms to be effective, their development should include a broader set of stakeholders, from private sector and civil society. Their various perspectives and expertise would add value to the process and the eventual outcome of any new conversations. In order to maximize security in cyberspace, organizations across all sectors should cooperate to ensure mutual protection from attacks by states, criminal groups, and terrorist organizations.

Indeed, a variety of non-state stakeholders have already proposed cybersecurity norms. Notable examples of efforts significantly contributing to our understanding of normative expectations in cyberspace include the work of the Global Commission on the Stability of Cyberspace (GCSC), as well as the proposal by some companies of norms for both private and public sector entities.

[9] Microsoft, 23 June 2016: Cybersecurity norms for nation-states and the global ICT industry. Available at: https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/#sm.0000uv1naaq41db5qsf12kuqx1j4m

GCSC is in the process of developing a set of recommendations on how to ensure the core of the internet is protected, and is expected to elaborate on other issues raised in relations to 2015 UNGGE in the coming months. This first set of recommendations, set to be revealed at the 2017 Global Conference on Cyber Space (GCCS) in Delhi, India, will help global players as well as local utilities speak the same language when it comes to protecting core national and international systems.

Industry is also interested in promoting cybersecurity norms, which has been expressed in the broad industry support for the 2015 UNGGE norms. In many countries, the vast majority of infrastructure is held by private companies. Worldwide, critical systems use private industry's software, hardware, and services. Industry therefore has an important role to play in enhancing cybersecurity and should be a partner for governments in the development of cybersecurity standards, norms, and policies. The norms suggested by industry can shape and inform how governments act in cyberspace, and vice versa. Proponents of this approach hope that an iterative and constructive dialogue aimed at building a long-term conversation on cybersecurity norms will lead to improved understanding and generate opportunities for collaboration.

In one example, Microsoft's recent publication cybersecurity norms lays out proposals (to maintain trust, establish a coordinated approach to vulnerability handling, stop proliferation of vulnerabilities, mitigate the impact of nation-state attacks, prevent mass events, support response efforts, and patch customers globally[9]) and the responsibilities of states alongside those of the global ICT industry. By examining the norms side-by-side, it is easier to find opportunities for collaboration and virtuous cycles which can foster better global cybersecurity.

Finally, because global consensus on cybersecurity norms is unlikely to materialize in the near term, it is worth noting that regional agreements on cybersecurity norms are being developed[10]. These agreements should be studied by all states, and may provide suitable frameworks for considering other norms that could be adopted. An interesting example of this is the Asia Pacific Computer Emergency Response Team (APCERT), which conducts capacity building and information sharing for CERTS from more than 20 countries in the region. It also coordinates with other regional CERTS (for example, in Europe and the Organization of Islamic Cooperation). One important facet of APCERT's work is the assistance it provides governments on addressing legal issues related to cyber security incidents and transnational incident response. It's work enables rapid sharing of information, by trained experts, about cyber-attacks among those countries who have agreed to work together. This, coupled with regional cybersecurity capacity building activities like the annual ASEAN CERT Incident Drills (ACID), will ensure that regional stakeholders are able to contribute to and benefit from improved cybersecurity. The development of processes and relationships in this forum will lead to de facto norms for how states cooperate in a mutual defense arrangement.

As the development of norms evolves from strictly multilateral, intergovernmental arrangements to multistakeholder ones, there will remain a need for harmonization of the implementation of norms between groups with similar geographic or economic considerations, and for capturing the best practices in their development. Doing so will enable the continued building of confidence in the norms system, leading to reduced tension and conflict in cyberspace.

[10] Carnegie Endowment for International Peace: "Cyber Norms Index." Available at: http://carnegieendowment.org/publications/interactive/cybernorms

RECOMMENDATIONS FOR CYBER NORMS IN SOUTHEAST ASIA

We have discussed the potential value that collaborative norms can provide for international security and stability, social and economic development, and the promotion of digital transformation. Within the context of the Southeast Asian region, several norms and related activities present themselves as potential next steps for the region to consider:

1. ESTABLISH A GLOSSARY

A common lexicon of cybersecurity terminology would likely help improve collaboration by facilitating the communication of computer emergency response teams and governments when facing common threats. This can be done in coordination with other organizations working on similar glossary, such as the OSCE.

In addition to helping emergency response teams, a common definition of the most pressing terms would also help the harmonization of laws between countries in the region and globally, which would aid businesses in understanding how to operate in the region's various markets, spurring investment and helping to bridge the digital divides that are major obstacles to the region's development.

2. COORDINATED VULNERABILITY DISCLOSURE AND MANAGEMENT

Governments in Southeast Asia should work with industry and other stakeholders to develop policies for coordinated vulnerability disclosure in systems and hardware. When industry is made aware of vulnerabilities and can issue patches before the vulnerability is made public, it improves the security of all users. This is reflected in the norms recommended by the UNGGE in 2015, which calls on states to encourage reporting of vulnerabilities and sharing of remedies to them.

Government's role in vulnerability handling is multifaceted. First and foremost, governments are central to initiating and encouraging voluntary cybersecurity information sharing activities by ensuring organizations that share information are not subject to any unreasonable legal or policy barriers. Similarly, they can advance the work of security researchers by creating frameworks that address intent or clarify acceptable research behavior.

3. COOPERATIVE INFORMATION EXCHANGE

The 2015 UNGGE report calls for States to "consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats." Within the context of the ARF, governments and other stakeholders may consider establishing guidelines for sharing of cyber threat information between governments, industry, and other affected stakeholders.

[11] Consensus Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22 July 2015. Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

This can be done in conjunction with FIRST and other global incident response coordinators, based on established international standards.

For an ARF-based information sharing mechanism to succeed, it should be built from the beginning as an open environment that can receive and transmit information to all relevant parties, while ensuring quality and rapid dissemination of information. This would help ensure that the entire region has the opportunity to collaborate and benefit from improved cyber hygiene at all levels of the region's economies.

4. BUILDING CAPACITY FOR THE REGION

One key, if somewhat overlooked, part of the 2013 UNGGE report called for the international community to work together to improve ICT infrastructure security, develop technical skills, and advise on legislative and policy issues. Building on this, the 2015 report states that "The development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach.[11]"

When governments do not have sufficient capacity in this regard, it can lead to greater vulnerability for citizens and government systems, and create safe havens for malicious actors. By providing mutual assistance, cooperation, and collaboration, states can exchange experiences, expertise, and strategies to improve the region's cybersecurity.

Capacity building as outlined by the 2015 UNGGE report includes a variety of activities that can benefit from the inclusion of all stakeholders. These include fostering cooperation mechanisms between CERTs, the exchange of legal and administrative best practices, creating procedures for mutual assistance in short-term situations and expedited assistance in case of emergencies, as well as prioritizing ICT security awareness and capacity building in national plans and budgets, in conjunction with other stakeholders.

The South East Asian region stands to benefit from building a regional approach to capacity building by identifying shared cultural, technical, and economic concerns around which to frame its capacity-building efforts.

Working together as a region, ASEAN member states can be a strong and unified voice in the global cybersecurity discussion, ensure a more secure cyberspace for their citizens, and amplify the social and economic benefits of digital transformation.

IMPORTANT DISCLAIMER

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the document is not offered in relation to the publisher rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

Published by: Access Partnership, Ltd
Tel: +1-202-503-1570
Email: ap.reception@accesspartnership.com
Web: www.accesspartnership.com

WITH SPECIAL THANKS TO THE CYBER SECURITY AGENCY, SINGAPORE.