UNIDIR

Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN

Report of the 2nd International Security Cyber Workshop Series

Singapore, 20–21 September 2017

United Nations Institute for Disarmament Research &
the Center for Strategic and International Studies

UNIDIR RESOURCES

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. In addition, dedicated funding for this project was received from the Governments of Germany and the Netherlands. The Singapore Cyber Security Agency provided in-kind support for the workshop held in Singapore on 20-21 September 2017.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to the variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and governments. UNIDIR's activities are funded by contributions from governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The views expressed in this publication are the sole responsibility of UNIDIR. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR's sponsors.

www.unidir.org

Contents

Executive Summary **1**

Workshop Summary..**3**

I. The 2017 GGE and Issues for International Agreement 3

II. Sovereignty and Global Perspectives on International Law for Cyberspace 4

III. Regional Perspectives on Norms and Confidence-Building Measures 6

IV. Regional Perspectives on Next Steps for International Cooperation 7

Executive Summary

The United Nations Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security are to date the only multilateral forums where States address cyber issues in the context of international peace and security.[1] However, the last GGE concluded its work in June 2017 without reaching consensus[2] and many question the future of the GGE process. With its limited membership, private meetings and consensus rule, some ask whether the GGE format should give way to a more transparent process with wider membership, or whether to continue with this format which has set important milestones for international cooperation on security issues in cyberspace. Regardless of the future format of the discussions, all States have a stake in cyber stability and there is a particular need to ensure that those States that have not previously served in GGEs understand the issues, the accomplishments and the challenges remaining—and are prepared to participate in the international discussion going forward—in whatever format it takes.

Building on the success of their 2016 workshop series on international norms,[3] the United Nations Institute for Disarmament Research (UNIDIR) and the Center for Strategic and International Studies (CSIS) are continuing the series with a particular emphasis on regional approaches and perspectives.

The first workshop in the series focused on the members of the Association of South East Asian Nations (ASEAN) and was hosted by the Singapore Cyber Security Agency, on 20-21 September 2017 on the margins of Singapore International Cyber Week. The workshop took place following the Second ASEAN Ministerial Conference on Cybersecurity (AMCC) and other high-level dialogues with non-ASEAN members, including Australia, China, Japan, New Zealand and the United States. At the AMCC, ASEAN formally adopted the existing eleven non-binding norms proposed by the 2015 UN GGE[4] as part of wider regional stabilization efforts. ASEAN has adopted a consensus-seeking approach to advancing cybersecurity norms, in keeping with the diverse philosophies and priorities of ASEAN members.

Despite steady progress at the regional level within Asia, there remains a wide disparity of capacity and interest in cyber security matters at the national level. To narrow this gap, more needs to be done to communicate the importance of regional cooperation on—and the responsibility of all States in—ensuring stability and security in cyberspace. While information and communication technologies (ICTs) clearly produce positive economic and social benefits, States must be realistic about the opportunities for misuse that can lead to destabilizing or escalatory behaviour.

Although the workshop's host Singapore has not been a member of any of the GGEs so far, its understanding of the challenges emanating from the cyber domain, and its maturity across technical, legal, and policy domains, make it a credible advocate for greater cyber cooperation in the region. Singapore is an active participant in regional and intra-regional discussions to build trust, resiliency and cooperation among States and the private sector on ICT issues.

The workshop brought together over 80 participants from the region and beyond. Representatives of 9 of the 10 members of ASEAN—Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Viet Nam—were present at the workshop,[5] as well as representatives from ASEAN Regional

[1] The three consensus reports of the GGEs are contained within UN documents A/65/201, A/68/98*, and A/70/174.

[2] See United Nations document A/72/327 of 17 August 2017.

[3] See http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

[4] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN Document A/70/174, 22 July 2015.

[5] Brunei Darussalam did not attend.

Forum (ARF) members, including Australia, China, Japan, New Zealand, and the United States. Seven experts from the GGE process also participated.

Representatives from the private sector, technical organizations, non-governmental organizations (NGOs) and academia from the region were active contributors to the workshop. The involvement of non-governmental stakeholders was considered valuable by all participants. Their views helped inform discussion on the role of private companies and civil society in a changing international security environment and brought perspectives to the discussion that have been absent from the GGE process due to its closed-door nature.

Key points that emerged during the workshop included:

- Participants recognized that while the economic diversity and differences in national values and governance structures present a unique challenge in the Asia Pacific region, the GGE norms were flexible enough to be adopted for all national contexts and that new, regionally specific norms are unnecessary. **Existing GGE recommendations should continue to function as a roadmap for States in the region, while regional forums can serve as platforms to operationalize these existing norms, as well as confidence-building measures (CBMs) and capacity-building efforts.**

- Mirroring debates within the GGE itself, much discussion at the workshop centred around the question of sovereignty. Experts and governmental representatives agreed that States will not cede the roles they play in creating frameworks for managing conflicts and security challenges. Technological development has not eroded States' traditional role in peace and security issues. Although a new doctrine is emerging around principles of State responsibility in cyberspace, it has not fully matured. States should be held responsible for ensuring that cyber capabilities are developed and used in a manner consistent with existing International Humanitarian Law (IHL). The challenge for ASEAN States is to find the appropriate framework for managing threats below the threshold of armed conflict in a region where geopolitical and economic competition can lead to miscalculation, and where existing tensions exacerbate the threat of cyber conflict. **In the absence of agreement on rules of engagement, States should borrow from past successes at building regional cooperation in non-cyber domains to improve transparency and coordination.**

- Regionally appropriate cyber CBMs should build on the work of the AMCC and the ASEAN Defence Ministers Meeting (ADMM). **While the focus of these efforts thus far has been on elevating technical capacity, future efforts should build policy and legal capacity among States as well.**

- **Regional venues for dialogue and capacity building in cyberspace should not occur in a silo from existing international efforts.** Progress on bridging the differences on international law issues will require significant diplomatic buy-in from large and medium-sized States, and success is far from guaranteed. Decoupling the non-consensus issues of international law from other areas of agreement allows States to move forward with the implementation of the agreed upon norms, build technical, legal, and policy expertise, and construct a more stable and resilient cyber architecture.

Workshop Summary

The workshop addressed four themes to capture regional concerns, opportunities and approaches in the context of international peace and security efforts in cyberspace:

- *The 2017 GGE and Issues for International Agreement;*
- *Sovereignty and Global Perspectives on International Law for Cyberspace*;
- *Regional Perspectives on Norms and Confidence-Building Measures; and*
- *Next Steps for International Cooperation.*

Many of the speakers emphasized that the failure of the GGE to reach consensus in 2017 was not a catastrophe. The GGE process since 2004 has met one of its objectives: to build awareness and understanding of peace and security issues in cyberspace. The GGE model may have outlived the issue of awareness raising, or the issues themselves may have outgrown the existing GGE construct.

With progress on cyber issues currently stalled within the UN General Assembly's First Committee, the previous UN GGE reports remain a solid starting point. States should consider how implementation of these recommendations could be best supported at the regional and national levels. The significant decision by the Second ASEAN Ministerial Conference on Cybersecurity to formally adopt the eleven 2015 GGE norms sets the stage regionally to do so. It is time to build regional expertise through specialized bodies on security, technical, and legal issues in order to transition from raising awareness to implementation.

I. The 2017 GGE and Issues for International Agreement

There was wide agreement among speakers that the 2017 GGE's inability to arrive at a consensus does not mean that the GGE process should be completely abandoned or that previous reports and recommendations welcomed by the UN General Assembly should be dismissed. The deterioration of the geopolitical environment since the successful 2015 GGE has widened the gap between States on key issues relating to ICT governance. Experts who had participated in the 2017 GGE assessed that there was near-agreement within the group on threat analysis, non-binding measures, capacity-building initiatives, and CBMs. They considered that the primary disagreements were over the applicability of existing international law to ICTs and on how voluntary, non-binding norms can help define responsible State behaviour.

While the outcome of the 2017 GGE reflects recent shifts in State behaviour and geopolitical tensions, it does not necessarily reflect an ideological divergence. Speakers remarked that international law is often leveraged for political purposes following changes in geopolitical circumstances. The rapid pace of technological evolution leaves open the possibility that States alter their bottom line during negotiation or change their views entirely on a particular issue as the implications for their country change. Further, speakers noted that the failure of the 2017 GGE to reach a consensus was ultimately the result of a lack of political will.

Norms in and of themselves do not prevent conflict; the willingness of States to enforce them does. Speakers remarked that norms serve a preventative function. Their purpose is not to restrict ICT use (in an arms control sense), but to help prevent and manage conflict between States. The eleven non-binding norms of 2015 provide organizing principles for like-minded States, but there will continue to be actors engaging in destabilizing behaviour during peacetime.

What was clear from the workshop discussion is that there remain several questions around defining the use of force in a cyber context. Some speakers noted that while they were unable to define the use of force, they would "know it when [they] saw it" and that States were entitled to take appropriate defensive actions in response. Others felt that a definition was immaterial and the guiding principle for action should be based on the observable effect of an attack. This raised further questions about the appropriate response to coercive actions below the threshold of armed conflict — "grey zone" activities that include information operations. Speakers agreed that self-defence was the prerogative of sovereign States and that such actions must be evaluated on a case-by-case basis. In extending that principle to cyberspace, one speaker noted that governments should be weary of limiting their response options by setting higher standards for actions in cyberspace than they do in physical domains.

Speakers noted that as States discuss next steps they should keep in mind that the GGEs were an abnormality in the sense that GGEs are usually limited to one or two occurrences on a particular theme and not a reoccurring process over a decade. For this reason, there might be a divergence between the stated international goals of widespread norm adoption and the structure of a limited and changing GGE membership.

Additionally, States need multiple channels—bilateral, multilateral (regional), and international—to help bolster trust and confidence. The multi-stakeholder approach must be inclusive and unify regional efforts with existing multilateral processes. Speakers remarked at the asymmetry of information that existed between the 25 GGE members and those outside the process. In order to build an open, stable and secure ICT environment, a greater number of States must feel engaged and listened to in ICT discussions on international security issues. Numerous States are already credible and capable partners in meeting collective security challenges related to the misuse of ICTs. It is essential that the number of States that are interested and capable of engaging on these issues continues to grow, while concurrently capacity is built in those States who have further to go before feeling able to fully participate in the discussion.

While it is unlikely that the 72nd session of the General Assembly will call for the establishment of a new GGE, this should not in itself be seen as "the end of the process" at the United Nations. Rather it is likely a reflection that the current international environment may not be conducive to productive engagement on these issues. Instead of forcing a consensus-based process in these inauspicious circumstances, focusing on universalizing buy-in on the existing norms, CBMs and cooperative measures as well as concrete action on operationalizing them at the national and regional levels would be a productive and useful step.

II. Sovereignty and Global Perspectives on International Law for Cyberspace

In the second session, panellists cautioned against using the 2017 GGE's failure to reach consensus as an excuse by States to "pull back" from multilateralism. Rather, it highlights the urgency to widen participation and engagement at the regional level in order to create a larger constituency for international engagement.

During this session, speakers noted that while existing IHL does not explicitly mention "cyber attacks", IHL principles such as *distinction*, *proportionality* and *military necessity* as well as other rules that govern the conduct of hostilities by States during a conflict apply in the cyber domain — even when these actions take place on closed networks. The most dangerous cyber operations are also the most precise, and the onus is on States to ensure that these new capabilities remain in compliance with existing international law and doctrine. While use of ICTs for military purposes is consistent with State sovereignty, a few participants expressed the view that countries with advanced cyber tools are not prepared to place them within a framework of international law and norms, or even willing disclose their existence. Increased transparency on cyber capabilities is a first step to building confidence, predictability, and stability in cyberspace; it allows States to preserve their sovereign rights and ensure that response options are clear and fall within the correct restraints on State action.

Speakers generally agreed that there is not a “vacuum” in international law as it applies to the conduct of hostilities in cyberspace and other domains. As a result, there is no explicit need to establish new treaties or conventions, and cautioned against setting higher standards for State behaviour in cyberspace than in other domains. Existing doctrine on countermeasures and other activities below the use of force, including sanctions and other diplomatic measures and tools that are proportional, timely and reversible is one such example. The doctrine of State responsibility too is an emerging area that may be applied to future activities in cyberspace. Speakers noted the utility of looking for guidance in other areas of international law that govern issues such as trade and human rights to inform approaches to the impact of ICTs across multiple domains.

The primary challenge for the international community is governing activities that are below the threshold of the use of force and that take place during peacetime (for example, activities by proxies, organized cybercrime networks, or botnets). It is necessary to preserve the distinction between frameworks that govern the use of force and other norms.

Private companies are now able to publish analysis on the sources and types of cyber attacks taking place on civilian networks. States are no longer the sole owners of this information, and in many cases lag behind the private sector in their analytical capability. While there are opportunities for the private sector and governments to work more closely together on international security ramifications of ICTs, speakers noted that progress on technical attribution will not necessarily lead to agreement on how to apply international law in cyberspace. There are examples in the kinetic space where actions taken were clear and attributable but did not illicit a response from the international community. Enhanced attribution in cyberspace, while technically feasible, cannot produce a standard that should guide State response absent other political and diplomatic considerations.

There was disagreement among participants on whether the fundamental question of governance should only address questions of harm/effect or tools/vectors. As cyber platforms have civilian and military uses, there needs to be more clarity on exactly what activities need to be subject to regulation, and what infrastructure should be explicitly protected. For now, there may be agreement on legal frameworks that allow countries to address transnational challenges such as cybercrime, but agreement on rules of engagement in cyberspace continue to be elusive—even at the regional level.

In light of the outcome of the 2017 GGE, regional participants raised the question of the political will of States to adhere to existing legal norms. Fostering political agreement among States is often more challenging than getting agreement on the application of international law. It was pointed out that the Tallinn Manual and similar efforts to develop interpretations of international law on matters related to cyberspace are useful but do not fully capture dynamics in international politics. When attacks or cyber incidents go beyond the intention of the originator, as is more likely to happen with cyber tools, nations must have relevant expertise to exercise political judgement and discretion when calibrating a response. This is also true of intentional attacks that are intended to be politically coercive and fall below the threshold of the use of force. Therefore, speakers noted that developing fixed, overly legalistic responses to provocations may not always be in the interest of States—and insistence on doing so may in fact have the unfortunate effect of hindering agreement or progress in other important areas.

Both governmental and non-governmental experts expressed scepticism about the prospect for establishing a permanent international cyber agency or institution. Many States are still in the early stages of building institutional and legal architectures for transboundary cyber issues. For cyberspace, the governance framework on which to build an institution—whether under the UN, modelled after the International Atomic Energy Agency (IAEA), or an entirely new body—does not yet exist. The current geopolitical environment and declining trust among States also indicates that more formal institutions have poor prospects. The absence of a centralized institution or universal declaration does not signal failure, though. On international cyber issues, there has been much progress made to enlarge the GGE process and socialize its recommendations in the G7, G20, and through other multilateral bodies. In the absence of a formal institution, speakers suggested that learning from the experience of governance in other domains such as outer space to improve coordination mechanisms could be a productive approach.

III. Regional Perspectives on Norms and Confidence-Building Measures

The Asia Pacific is a unique environment for cybersecurity issues. The region is economically diverse, and is home to approximately fifty percent of the world's total Internet users.[6] However, it is a region of asymmetries. More than half of households do not have Internet access. Many countries in the region are rushing to bridge the "digital divide", improve connectivity, and get their citizens online as quickly as possible. This has led many States to ignore or deprioritize consideration of cybersecurity risks. In addition, differences in national values and governance structures, coupled with strong and diverse views on issues such as sovereignty, human rights, and content control, are crucial facets of the regional discussion that should not be underestimated.

There was strong disagreement among workshop participants on whether the GGE process was flexible enough to accommodate the cultural diversity of States. While some criticized the eleven norms from 2015 for being "vague", others insisted that they were deliberately crafted as such in recognition of different national contexts. Still, it was clear that participants from the ASEAN region are seeking to have a frank discussion on content control issues specifically, something that the GGEs have thus far not been able to agree upon.

The Asia Pacific is also a region where building trust among neighbours remains crucial. Strategic competition among regional rivals and other geopolitical considerations will shape the willingness of these States to voluntarily coordinate on cyber issues. The rise of new political and economic powers in Asia will impact existing international governance frameworks and perhaps even the feasibility of developing new international norms and CBMs.

The GGE reports have served as a roadmap by offering ASEAN States high-level commitments that set expectations for responsible State behaviour. However, even with high-level principles in place, existing asymmetries in technical, legal and political cyber expertise and cyber capability are obstacles to deepening trust among States. Speakers also noted that difficulties associated with attribution make building trust more challenging.

In order to shape behaviour, norms need to be created (or recognized), diffused, and internalized by States. There was recognition among speakers and participants that the GGEs have been successful at creating norms, and that regional stakeholders might be better leveraged for propagating them. Yet, regional experts in the room noted that the view in ASEAN five years ago was that cybersecurity and cyber norms were issues for major powers in the international community, and that cybersecurity was a technical domain beyond the reach of policy and diplomacy. The priority of regional policymakers was stimulating the emerging digital economy. The adoption of the 2015 GGE norms by the ASEAN Ministerial Conference on Cybersecurity thus marks a significant turning point in this understanding and is an opportunity that those wishing to build capacity and momentum on cybersecurity issues in the region cannot afford to miss.

[6] See APNET, *Digital 2017: Asia Pacific Regional Overview*, https://datareportal.com/reports/digital-2017-apac-regional-overview.

In ASEAN, information silos also contributed to institutional and structural challenges for communication and multilateral efforts. Responsibilities for cyber in the region were either non-existent or spread across various ministries—defence, trade, information communications, foreign affairs, and intelligence. This results in competing internal interests and retards regional and international engagement.

Speakers agreed that awareness about the work of the GGE has been successfully raised during ASEAN ministerial meetings and other regional forums. These priorities are reflected in the inclusion of cyber issues in the ASEAN Defence Ministers Meeting agenda, the ASEAN Regional Forum, and in official statements made by policymakers in the region. The focus of regional level meetings should now turn to operationalization, and to improving coordination among States to ensure that regional measures are complementary and reinforcing.

There has been steady progress on building regional capacity and forming a community of practitioners. Speakers recognized that the current geopolitical environment might mean legal and technical capacity building is likely to continue to be prioritized over political and diplomatic progress—however, States in the region should be encouraged to use the likely hiatus in the GGE process to build internal political capacity in order to be poised to actively participate in international cyber discussions once they reconvene. This point that capacity building should be expanded beyond regional and national CERTs (Computer Emergency Response Teams) to include policy-planning staff was echoed by several speakers and participants throughout the workshop. Higher capacity States could prioritize helping their neighbours develop such a policy-focused capacity and the national political structures necessary to support it.

Greater maturity on legal and technical matters can also enable States to be more forward-thinking and proactive on supporting norms and CBMs. The comprehensive cooperation strategy that followed the AMCC also demonstrates progress on implementation. To build on this momentum and progress to date, Singapore has committed to improving coordination and reducing duplication of cyber capacity-building efforts a priority during its chairmanship of ASEAN in 2018.

IV. Regional Perspectives on Next Steps for International Cooperation

Today, between eighty and ninety countries are in the process of drafting or revising their cybersecurity laws.[7] There are also approximately thirty countries who have actively invested in offensive capabilities.[8] Speakers and participants agreed that there is increased urgency to deepen international engagement and cooperation; some characterized it as governments are increasingly acting in the cyber domain and considering the consequences after. The goal should be to build a more resilient cyber architecture for both times of peacetime and times of conflict; one that strikes an appropriate balance between social and economic opportunity, and cybersecurity. What was clear is that progress on these issues cannot be limited to a single forum, nor can it replace the existing international discussion on norms.

The pause in the GGE process also offers the opportunity to explore other venues for cooperation on cyber issues beyond the UN. Alternative venues for dialogue would allow for a wider participation of non-governmental stakeholder communities, as has been the case with the Tallinn Manual and Hague Process. While States may not always agree with the conclusions drawn or recommendations by non-governmental experts (including the private sector), multi-stakeholder participation can lead to a more informed debate on

[7] "Global Cyber Strategies Index," Center for Strategic and International Studies, n.d., https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/global-cyber-strategies-index.

[8] James R. Clapper, Marcel Lettre, Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee on Foreign Cyber Threats to the United States," January 5, 2017, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

international law and cyber governance. This “socialization” works both ways: States are exposed to and have an opportunity to consider the views, suggestions and concerns of citizens and industry, and conversely, non-governmental experts have a chance to deepen their appreciation of the political and legal constraints and considerations that they may be unaware of.

The Global Conference on Cyberspace (GCCS or “London Process”) is another example of a multi-stakeholder effort to raise awareness and harmonize government and industry recommendations to improve trust and transparency. Following the 2017 GCCS in India, States should also consider how the international community can better leverage the GCCS to focus on the operationalization of the GGE norms.

There was agreement among speakers and participants that there was some role for the private sector to play, but no consensus whether their role should be more clearly defined. Private companies find themselves in a unique and challenging position; their relationship to national governments have traditionally been viewed through a consumer, regulatory, or law enforcement lens. ICT products and services span multiple jurisdictions and simultaneously enable governments to execute economic and strategic objectives, and function as targets for exploitation and disruption by States. While there has been an increasing emphasis on public-private partnerships, private sector participants at the workshop noted that there are not many existing forums for governments and industry to engage in a substantive way on issues that include international law, the control of dual-use technologies, and principles to guide the use of new technologies.

At the end of the session, participants were asked to consider six potential formats and a variety of characteristics for taking forward the international discussion in order to see if there were any regional preferences. The options were:

- Another GGE
- A limited membership working group
- An Open-Ended Working Group
- The Conference on Disarmament
- The UN Disarmament Commission
- A Conference of States

The characteristics included membership rules, the mandate, the procedure for decision making, and the final output (a report, a treaty, recommendations, etc).

A majority of participants favoured the UN General Assembly as the most appropriate international venue for advancing on international cyber security. However, unlike in previous GGEs where the First Committee resolution mandate included exploration of how international law applies to ICTs—an issue that contributed to divisions in the 2017 GGE—the favoured proposal would decouple issues of implementation of the existing GGE recommendations from legal issues. In this proposal, the discussions on international law could take place in specialized bodies, such as the Sixth Committee of the General Assembly or the International Law Commission, while an *ad hoc* subcommittee could review implementation of recommendations made by previous GGEs. An informal consultation process open to all UN Member States would help to address the concerns that the GGE process has not been inclusive enough.

The majority of participants in the room felt that placing the non-consensus issues in a specialized body while concurrently building capacity in other areas may be the best that can be done in the current international environment.

It was remarked upon that in the options for taking forward multilateral discussion on cyber security, the private sector was noticeably absent. It was suggested to create a dialogue that runs in parallel to any newly established process in order to leverage the technical expertise of the private sector that is lacking in many governments. There is precedent for such a hybrid model: the Organization for Security and Co-operation in

Europe (OSCE) Security Committee's Informal Working Group on ICTs features government and private sector representatives. Comment periods on international proposals relating to the governance of ICTs and cyberspace that were open to the private sector were also raised as a possibility.

Also largely absent from the international security discussion are civil society groups. Unlike the robust and diverse civil society community focused on digital issues such as privacy, net neutrality and Internet governance, there is no equivalent civil society engagement on international cybersecurity issues—in ASEAN or elsewhere. Demonstrated civil society interest in the international security dimension could apply pressure on governments to continue all efforts for a more open, stable and secure cyberspace.

Speakers concluded that even if addressing non-consensus issues will require further debate, efforts to build regional capacity should continue to be encouraged. Speakers noted that any regionally-focused development or cooperation programme should make communicating the importance of cyber security a priority. Speakers made it clear that the international community has both the resources and the infrastructure to raise awareness and build capacity among policymakers. The question is identifying the right policymakers and convincing them that deeper engagement is in their national interest. Others noted that while the infrastructure may exist for diplomatic engagement on cyber issues, staff in these positions frequently rotate and lack expertise in multiple areas.

It was suggested that in order for cooperation to be successful, cyber diplomacy requires dedicated offices and experts. For ASEAN, this would also mean placing cybersecurity in the context of larger regional security issues and encouraging staff in the foreign and defence ministries to develop permanent expertise and structures. The private sector representatives at the workshop supported this framework, but raised the concern that capacity building is not scalable or sustainable. They will continue to advise on cybersecurity best practices and the development of national strategies, but anything beyond coordination may be out of reach. In addition, speakers emphasized that significant amounts of capacity building also needs to be done outside of the emerging economies in order to reduce vulnerabilities which create risks for the entire global Internet ecosystem.

Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN

Report of the 2nd International Security Cyber Workshop Series

Singapore, 20–21 September 2017

United Nations Institute for Disarmament Research &
the Center for Strategic and International Studies

Through a series of regionally focused workshops, the United Nations Institute for Disarmament Research and the Center for Strategic and International Studies are considering regional approaches and perspectives to building cybersecurity.

This workshop, the first in the series, brought together members of ASEAN and the ASEAN Regional Forum with representatives from the private sector, technical organizations, NGOs and academia to consider regional concerns, opportunities and approaches in the context of international peace and security efforts in cyberspace.

UNIDIR RESOURCES