UNIDIR

Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in the Americas

Report of the 2nd International Security Cyber Workshop Series

Washington, DC, 27 February 2018

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 General Secretariat of the Organization of American States offered an in-kind contribution for the hosting of this workshop.

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

The United Nations Groups of Governmental Experts (GGEs) 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 focused on the members of the Association of South East Asian Nations (ASEAN) and was hosted by the Singapore Cyber Security Agency, 20–21 September 2017 on the margins of Singapore International Cyber Week. The second workshop of the series was hosted by the Organization of American States (OAS) in Washington, DC on 27 February 2018.

The OAS has played an outsized role in facilitating regional cooperation on cybersecurity. The OAS membership is far more likeminded than not on cybersecurity issues, and on larger peace and security challenges relating to the use of information and communication technologies (ICTs). The OAS has been steadily improving the cybersecurity capacity of its members by helping to promote the understanding of norms and regional confidence-building measures (CBMs) proposed by the GGEs. The recommendations in the 2010, 2013, and 2015 GGE reports allowed States in the region to sharpen their focus on international cybersecurity issues.

American States have a wealth of experience combating cybercrime, which has helped governments and law enforcement officials to build the technical, legal, and operational capacity to confront emerging issues in the cyber landscape. Brazil, for instance, has introduced a number of initiatives to improve its cybersecurity capacity in preparation for the country's hosting of the 2016 Olympics and in the wake of multiple hacks on its financial institutions. Seventeen Latin American countries have established Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs),[4] and thirty-five countries are currently participating in capacity-building measures in conjunction with INTERPOL to improve training and operational coordination.[5]

[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] Inter-American Development Bank and the Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" March, 2016, https://publications.iadb.org/publications/english/document/Cybersecurity-Are-We-Ready-in-Latin-America-and-the-Caribbean.pdf.

[5] INTERPOL, "Cybercrime Capacity Building Project in the Americas," https://www.interpol.int/Crimes/Cybercrime/Cybercrime-training-for-police

The workshop brought together over 80 participants, with representatives from 20 member States of the OAS, as well as from five European countries. Three experts from the GGE process were among the participants. In addition, relevant international and regional organizations, including the Inter-American Defense Board, INTERPOL, the Office of the United Nations High Commissioner for Human Rights, the Organization for Security and Co-operation in Europe (OSCE) and the United Nations Office for Disarmament Affairs, were present.

Representatives from the private sector and non-governmental organizations (NGOs) also actively participated. Their views were considered a valuable contribution to better understanding of the roles and responsibilities of non-State actors in a changing international security environment.

Key points that emerged during the workshop included:

- Wide agreement that the lack of GGE consensus in 2017 offers an opportunity to be more ambitious with setting regional targets for implementation and devising alternative initiatives to improve peace and security in cyberspace.

- States in the Americas benefit from a strong regional organization, as well as existing laws, norms and experience with regional cooperation and CBMs. Together these form a framework to address challenges such as cybercrime and critical infrastructure vulnerabilities.

- Throughout the workshop, the interventions by governmental participants demonstrated that regional consensus is starting to coalesce around a more comprehensive concept, “digital security”, which includes cybersecurity and cross-border data issues. Digital security also encompasses how ICTs impact physical spaces.

- On larger strategic issues, speakers noted that countries of the Americas other than the United States are not immune to information warfare. The challenge for States will be to develop tools and strategies for maintaining democratic norms while constraining illegitimate or malicious exploitation of cyberspace. Speakers suggested that in the current international environment, interest-based approaches for improving cybersecurity, rather than values-based arguments, may resonate better with sceptical States and stakeholders.

- The OAS region is further advanced than many others in its willingness to consider the role of law enforcement in improving cybersecurity, and potential areas of cooperation between law enforcement bodies, industry, and civil society.

- While generally optimistic about future prospects for progress at the international level, participants cautioned that inaction by likeminded States during this post-GGE period of transition could cede the ground to authoritarian views on Internet governance.

- Regional perspectives of next steps at the international level echoed many of the themes heard from ASEAN countries at the first workshop[6]—with preference for a small working group to be established by the First Committee of the United Nations General Assembly.

[6] See UNIDIR–CSIS, *Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches,* Report of the 2nd International Security Cyber Workshop Series, Singapore, 20–21 September 2017.

Workshop Summary

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

- *The Global Cyber Environment: Risk, Crime, Governance and State Behaviour*;
- *How Norms Build Confidence and Stability; and*
- *The Future of International Cybersecurity Negotiations.*

Session I. The Global Cyber Environment: Risk, Crime, Governance and State Behaviour

This session opened with speakers agreeing that cybercrime is the leading threat in the region, but that politically motivated activities that blend geopolitical and economic interests are on the rise. Low barriers to entry have opened the space for malicious actors from outside of the region to engage in these activities. One speaker noted that criminal networks in Eastern Europe are providing training services to criminal groups in Latin America, who view cybercrime as a low-risk activity compared to narcotrafficking and other illicit activities. Attacks without a clear (or singular) motivation that blend cyber and non-cyber means present a unique challenge. Speakers noted that combating efforts to interfere in and subvert the democratic process should be prioritized over the threat of State-sponsored and directed sabotage or espionage.

As the line between economically and politically motivated cyber incidents is increasingly blurred, speakers urged the need to further distinguish between cybersecurity and cybercrime. Although WannaCry, NotPetya, and other large-scale ransomware attacks can involve multiple jurisdictions, they are first and foremost a technical challenge. When these incidents occur, implementing initial mitigation measures are addressed first by technicians, not law enforcement. "[Victims] want to patch their devices, not call the police," noted one of the speakers. The 2013 and 2015 GGE reports called for additional efforts to bridge the gap between States and the technical cybersecurity and law enforcement communities through, for example, strengthened practical cooperation—and clearly more should be done to bridge this gap.

Cooperation on law enforcement issues at the regional level in the Americas is excellent and continues to improve. For example, cooperation between the United States Secret Service and Costa Rica's Judicial Investigation Organization led to the arrest and prosecution of the founder of Liberty Reserve, a sizable virtual currency and money-laundering hub used by criminals to monetize their illicit activities. Although direct collaboration on an investigation may not always be possible—due to resource constraints, uncertain or conflicting authorities between intelligence and law enforcement bodies (e.g. in the event of a State-sponsored attack) or other limiting factors—there are other steps law enforcement bodies can take to foster constructive relationships and improve coordination at the regional level. INTERPOL, for example, provides its members access to analytical tools and resources, and conducts seminars and workshops to raise cyber awareness and improve operational capacity and coordination. The panel agreed that productive engagement necessarily requires building capacity, not just using States as conduits for information sharing.

A related theme that emerged throughout the session was the need to bridge the gap between ensuring national security (the responsibility of national governments) and addressing criminality (the responsibility of law enforcement). A growing number of challenges facing the region sit between traditional law enforcement and defence issues, requiring new strategies for preventing and mitigating threats. Greater awareness can lead to greater respect for existing laws and norms, but also improved collaboration, innovation on new solutions, more efficient resource pooling and allocation, and opportunities for States to learn best practices from one another. Given the hybrid nature of the cyber threat and the likelihood of deeper engagement between States on cyber issues, efforts to build diplomatic capacity and expertise should be given equal attention. Speakers noted that the norm of State responsibility is becoming more important as the victims of malicious cyber activities increasingly expect countries to take action to confront illicit activities emanating from within their borders.

Interestingly, government representatives seemed most concerned with improving their relationship with the private sector, notably domestic Internet service providers, rather than improving interstate cooperation. Many participants noted that providers are not proactively sharing network information and reporting illicit traffic on their networks. Further, service providers in the region lag in reporting breaches and other cyber incidents to law enforcement officials and other relevant bodies. The panel remarked that efforts to collect information about known vulnerabilities was equally important as tracking the attacks emanating from outside their borders. Further, the panellists suggested that focusing on shared interests between law enforcement and the private sector in informal conversations would yield better results than bringing in sector regulators. Government entities need to communicate their priorities to influence service providers and private entities outside their direct control. As one speaker noted, this approach is also consistent with conversations about Internet governance and the shift away from a values-based approach to an interest-based approach. Lastly, speakers remarked that States should recognize the inherent tension between commercial and privacy interests and the needs of security and law enforcement agencies is healthy for democracy, encouraging debate and awareness over competing priorities and ultimately leading to better security outcomes.

Throughout the discussion, governmental participants raised questions about managing inconsistencies between States' definitions for cyber incidents and threats, and the legal mechanisms that apply in different situations. Speakers noted that a holistic approach was needed to improve cyber awareness and resilience. This includes traditional stakeholders—national CERT teams, service providers, and law enforcement bodies—that handle cross-border data issues, and judges, prosecutors, key government ministries, and elements of civil society. One speaker noted that seeking standardization for definitions (e.g. on what constitutes "cyber war") would likely be unproductive, but emphasized the need for States to actively share national terminology, laws, and other relevant guiding principles as a CBM, as was recommended by the 2015 GGE.

The variety of different legal systems present in the region poses a challenge to increasing cooperation. Aside from the differences between common and civil law societies, there are no widespread standards in Latin America for which cyber-enabled activities are criminalized. This is made more difficult by differences in the maturity of legal regimes in the region and their ability to adequately adjudicate questions related to digital evidence, privacy, and cybersecurity. One speaker noted that the Budapest Convention represents a "floor" for what constitutes criminality, but that more robust measures would have to be pursued by States. Participants also noted that existing international norms, and the degree to which law enforcement bodies (including judges) adhere to them, must also be considered when legislating criminality and cooperating on cross-border cyber issues. And although norms and CBMs are often framed and perceived as applying primarily to diplomatic and security officials, one panellist noted that these should also be thought of as pertaining to law enforcement bodies.

Session II. How Norms Build Confidence and Stability

Despite the UN General Assembly's call that Member States should be guided in their behaviour by the 2015 GGE report recommendations, the speakers noted that there remain important challenges in implementation of these norms. The conversation focused on improving regional capacity in three areas: norms implementation; crisis management; and diplomatic training. Speakers agreed that the focus should be on bolstering existing norms, CBMs, and multilateral processes. They noted that strengthening these pillars will allow the norm of State responsibility to become more widely promulgated—speakers and panellists viewed this norm as central to improving cooperation and security.

The GGE process has affirmed the application of existing international law to cyberspace, and has articulated specific limiting norms and positive duties to maintain a secure and peaceful ICT environment. Despite the 2017 GGE not reaching a consensus outcome, workshop participants noted that because norms are intended to supplement, not replace, States' understanding of international law, there was ample opportunity to build on the momentum of previous GGEs to communicate and socialize best practices with States and assess how GGE-endorsed norms, such as State responsibility, are reflected in existing national policies and practices.

Norms also provide standards that allow the international community to assess the activities of States. One panellist noted that norms limiting State behaviour are primarily reflected in national defence and intelligence documents, while positive norms have grown out of national legislative efforts and legal decisions. With that framework in mind, the speakers suggested that there was more progress that could be made on implementing positive norms, ranging from sharing information about ICT vulnerabilities and patches to improving cooperation among States to prosecute criminal and terrorist use of ICTs.

The panel noted that one positive norm that has seen increased attention is the security of critical infrastructure. Speakers noted that the critical infrastructure norm represents an opportunity to address cybersecurity challenges and improve cooperation across sectors and between nations. The emphasis on critical infrastructure fits in with efforts to deepen partnerships. This requires flexible national approaches, modernized legal frameworks (such as reciprocity arrangements) and policies to improve cooperation between government and industry. Operationalizing these norms can help improve response, protection, and detection of routine incidents, and lay the groundwork for better cooperation with other nations in the event of a large-scale attack.

Also in relation to partnerships, speakers noted that addressing and reporting vulnerabilities is attracting increasing attention. Governments have a role in helping to reduce risk due to vulnerabilities throughout the cyber ecosystem—whether through bug bounties or other incentive programs, formal reporting to vendors, or a policy such as the Vulnerabilities Equities Process (VEP) in the United States. Country representatives agreed with the principles related to improving the security of critical infrastructure, enhancing State cooperation, and reducing vulnerabilities in the ecosystem, but noted that establishing a constructive degree of transparency between industry and government remains a challenge in many countries in the region. Further, even if the private sector and government entities were willing to cooperate, country representatives remarked that government and industry stakeholders do not always have a clear roadmap for what they should do after a vulnerability is discovered and disclosed.

It was telling that government participants described their vision of improved cooperation and coordination with the private sector and technical communities in almost exclusively technical terms—automated threat indicator sharing, early warning systems, and improved network-mapping tools. While important, this shows that there is room for improving political and diplomatic capacity alongside technical solutions. One speaker noted that although progress has been made on this front, "cyber diplomacy" is still a new concept for many in the region.

Capacity-building efforts should not be limited to State-level engagement, either. Here, the examples of Colombia and Mexico in developing their national cyber strategies are illustrative. Both nations had experts in the 2017 GGE and were concurrently developing new national cyber strategies in coordination with the OAS. They consulted with key ministries, established inter-sectorial committees, and engaged with international partners as well as members of civil society to produce holistic, flexible strategies. Speakers noted that the robust dialogue among all the stakeholders consulted during the process laid a much more solid foundation for effective roll-out and implementation than had the strategies been developed in isolation. The iterative and inclusive processes that Colombia and Mexico used to craft their national strategies serve as useful roadmaps for other countries in the region.

There was general agreement that strengthening existing frameworks and processes should involve progress on implementing existing voluntary norms, in addition to identifying gaps where progress on legally binding measures may be feasible. Commitments, political or otherwise, will strengthen mechanisms to hold States accountable. The panel agreed that tying norms back to responsible State behaviour, using all the tools in the diplomatic toolkit, and working with industry and civil society on implementation, would make States more resilient and able to respond to threats, as well as foster a more secure ICT environment.

Session III. The Future of International Cybersecurity Negotiations

In this 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.).

Overall, workshop participants favoured the establishment of a limited membership working group established by the General Assembly First Committee, with a mandate to review the implementation of the recommendations put forward in the 2010, 2013, and 2015 GGE reports. The objective of the working group would be to adopt a consensus-based report. This process would involve regular intersessional consultations with the wider UN membership, offering more transparency and inclusivity than the traditional GGE format, thereby addressing the concerns by some in the region that the GGE process had been insufficiently representative. Some participants pointed to recent precedent for this format in the high-level fissile material cut-off treaty (FMCT) expert preparatory group established pursuant to resolution 71/259.[7]

Cybersecurity has moved up on the world's agenda, and speakers felt that there is an increased sense of urgency to move ahead with First Committee discussions on cybersecurity or else risk losing the UN as a credible venue for these issues. Participants remarked that the numerous politically motivated malicious cyber events of 2017 demonstrate that cyber is rapidly emerging as the domain of choice for political interference. The use of ICTs for subversion and manipulation of data is destabilizing and presents a

[7] Two informal consultative meetings were held in New York on 2–3 March 2017 and 15–16 February 2018.

troublesome trend. Experts at the workshop agreed that these trends only further confirm that the focus of like-minded States should continue to be the promotion and operationalization of existing norms while clarifying areas of international law that have not yet been addressed in the context of ICTs. Consideration of new conventions or treaties seemed to have little support among the participants in favour of emphasis on strengthening and building awareness so that regional organizations can then feed their findings back into the global process to maintain momentum on addressing cybersecurity challenges.

Participants expressed a desire for increased opportunities for stakeholders to work together on developing collective outcomes, such as norms and implementation guidelines. They also noted the dearth of cross-regional/cross-functional dialogues. Bringing communities with expertise in the defence, crime, and governance aspects of cybersecurity together would be useful to combat the limited vision that technical experts have concerning political constraints and realities, and vice versa. Industry seems more willing than ever before to engage in formal processes, although most of the drive is coming from large, predominately US-based tech companies—which do not enjoy universal trust by all States in the region.

Overall, the workshop participants agreed that the lack of consensus in the 2017 GGE should not be viewed as a failure. The existing GGE reports serve as an underutilized roadmap; they have the potential to be adapted and greatly expanded upon at the regional level. There is room for the OAS to play an even greater role in facilitating discussion and moving forward on norm implementation, capacity building, and cooperative measures. States in the region could do much more to improve cooperation among neighbours and allies, and between different expert communities (policy, technical and legal). National strategies are important, but they are just one metric of progress. Regional organizations and their members should continue to push to build capacity and improve coordination to enhance the region's ability to address future cyber threats and improve international cyber stability.

UNIDIR

Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in the Americas

Report of the 2nd International Security Cyber Workshop Series

Washington, DC, 27 February 2018

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 second in the series, brought together members of the Organization of American States 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