The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities

Report of the 2nd International Security Cyber Workshop Series
Geneva, Switzerland, 24 January 2019

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.

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 **5**

Regional Perspectives on Cybersecurity 5

Regional Best Practices and Cooperation 6

Overview of the GGE and OEWG Processes 8

International Perspectives on Regional Cooperation 9

Issues for International Dialogue 9

Conclusion 10

Executive Summary

The fifth United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security concluded its work in June 2017 without reaching consensus.[1] In the absence of a multilateral process, greater prominence has been given to the activities and achievements of regional organizations on cybersecurity issues. Regional organizations have actively assisted their members with the implementation of the recommendations of the 2010, 2013 and 2015 consensus reports of the GGEs by offering guidance, building capacity and helping to address cyber concerns in regionally appropriate ways.

At the 73rd Session of the United Nations General Assembly in 2018, Member States decided to establish a new GGE[2] as well as an Open-Ended Working Group (OEWG)[3] on security in the use of information and communications technologies, with work beginning in the second half of 2019 for each. Against this backdrop of preparations for the re-convening of multilateral discussions on cyber issues at the United Nations, the United Nations Institute for Disarmament Research (UNIDIR) and the Center for Strategic and International Studies (CSIS) held the workshop "The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities" in Geneva on 24 January 2019.[4]

It is hoped that the GGE and OEWG advance the international discussion of cybersecurity norms, rules and principles of responsible State behaviour; confidence-building measures (CBMs); and international cooperation. The OEWG in particular offers the opportunity for States that have not previously participated in a GGE to engage in the international discussion. However, many States still have little indigenous capacity or expertise on these issues. This is compounded by the low level of awareness concerning the progress made to-date on cybersecurity, including the three consensus GGE reports.[5]

Regional organizations have a unique and central role in helping to prepare and support their members' active participation in these discussions, implement already-agreed norms in ways that enhance regional stability and security, and lay the foundation for further progress at the multilateral level.

Regional cybersecurity efforts typically involve awareness building, capacity building, confidence building, and cooperation.

- **Awareness building**. In some States and regions, the value of cybersecurity remains underappreciated—despite the dependence of finance, transport, and other critical services on cyber networks and digital infrastructures. Regional organizations raise awareness of how cybersecurity can contribute to economic and social development and to the public safety objectives of interest to all States.
- **Capacity building**. Awareness tells policymakers what problems and risks they face; capacity building provides them with the tools to address these problems. As networks and data have become central

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

[2] A/RES/73/266 of 2 January 2019.

[3] A/RES/73/27 of 11 December 2018.

[4] This was the third and final workshop in a series examining regional approaches and perspectives to cybersecurity. The first workshop focused on the members of the Association of Southeast Asian Nations (ASEAN) and was hosted by the Singapore Cybersecurity Agency, 20–21 September 2017 on the margins of Singapore International Cyber Week. The second workshop targeted the Americas and was hosted by the Organization of American States (OAS) in Washington, DC on 27 February 2018. See http://www.unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

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

to economic, social, and political activities, capacity building cannot be limited to developing the technical skills needed for addressing data security and cybercrime but must include policy and legal expertise as well. Establishing the essential national organizational structures, strategies and procedures for cybersecurity requires policymakers equipped with the knowledge and tools to do so.

- **Confidence building**. Regional organizations have long traditions of building trust and confidence among their members, through information exchanges, joint activities, building relationships and establishing crisis communication mechanisms.
- **Cooperation**. While cyberspace is often considered "borderless", national actors are constrained by legal jurisdiction and respect for the sovereignty of other States. Developing the diplomatic and law enforcement tools needed to cooperate with other States and to participate effectively in global cybersecurity discussions cannot be neglected. At a minimum, a government needs to have responsive officials in law enforcement, security, and economic ministries who can work with other States and with the private sector.

Regional organizations are uniquely situated to assist their members in developing these capabilities. It is difficult to share doctrine and strategy (a standard CBM) if these do not exist, and cooperation is hampered if capacity and structures are lacking. Regional organizations offer a framework within which States can take a focused approach to these issues, yet can be tailored to the capacity and concerns of each State.

In order to consider how different regions have approached these roles and how they might develop going forward, UNIDIR and CSIS invited representatives from regional organizations, members of the diplomatic and international organization community in Geneva, national cyber authorities, the technical community, military advisors, think-tanks and research institutes, and civil society to discuss regional approaches to cybersecurity. Alongside expertise from the African Union (AU), the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE), the European Union (EU) and other regional organizations, over 120 participants engaged in the day's discussions.

Key points that emerged during the workshop included:

- Each region has **different social, economic and security priorities and challenges** and thus regional organizations have developed **regionally specific responses and resources**.

- **Each regional organization has different strengths and capacities**: the OAS's experience with developing a "cyber lab", the OSCE's leadership on development of CBMs, and ASEAN's success in building cooperative arrangements are examples of successful regional efforts that target the particular needs or priorities of different regions. Organizations that are only beginning to develop their cyber capacity can be inspired by these activities and adapt them to their own needs as appropriate.

- As the GGE recommendations concerning norms, information exchange, capacity building and other measures are voluntary, some of the most **effective mechanisms for implementation** are at the regional level.

- Regional approaches to cyber stability play a crucial **role in enhancing trust**. Cooperative measures within regional organizations and among them to share information and develop common responses can **build confidence** among States and improve the overall cyber environment.

- Regional forums also help **establish expectations for responsible State behaviour** among neighbours.

- Experts working on cyber issues within regional organizations have identified the need for greater **Peer-to-Peer exchanges** to discuss specific challenges, exchange ideas and share resources.

- By **sharing experiences, lessons learned and guidance**, organizations could build upon and adapt successful measures from other regions to their own contexts, or avoid costly mistakes.

Workshop Summary

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

- *Regional Perspectives on Cybersecurity;*
- *Regional Best Practices and Cooperation;*
- *An Overview of the GGE and OEWG Processes;*
- *International Perspectives on Regional Cooperation; and*
- *Issues for International Dialogue.*

Regional Perspectives on Cybersecurity

In order to set the scene for the day's discussions, the first session opened with experts from Asia, Africa and Latin America providing an overview of how their respective regions are thinking about cybersecurity policy, reflecting on the progress they have made in implementing norms and recommendations from the 2010, 2013 and 2015 GGE reports, and considering priorities for future work.

A common issue across regions is ensuring that cybersecurity is seen as a policy issue, and that there is sufficient awareness among policymakers and political leaders of the perils of ignoring cyber risks. In some regions the perception remains that cybersecurity is a technical issue, not a policy issue. All speakers agreed that cybersecurity cannot be left solely to technical experts. Policymakers have the responsibility to ensure the protection of critical infrastructure, prevent cybercrime and malicious acts, and foster a conducive atmosphere for economic growth—and thus must take an active role in cybersecurity.

Regional organizations have had some success in raising awareness among policymakers and leaders in their member States about cyber issues. For example, one speaker noted a correlation between progress made by Association of Southeast Asian Nations (ASEAN) members in adopting a strategy on cybersecurity cooperation,[6] their work implementing the GGE norms under Singapore's ASEAN chairmanship in 2018, and a greater interest in cybersecurity discussions within the governments of ASEAN members.

Speakers acknowledged that when trying to promote awareness within governments, regional organizations face the challenge of getting the attention of policymakers unless there is a perception of an imminent threat. For example, one cited that it was only after the Facebook-Cambridge Analytica scandal that Brazil resumed discussions on data protection and passed relevant legislation.[7] Lack of awareness, compounded by competing priorities for limited human and financial resources, results in policymakers who are ill-equipped to respond effectively when a cyber incident occurs.

Another shared perception across regions was that multi-stakeholder participation is critical in supporting cybersecurity efforts as regional organizations, industry, non-governmental organizations (NGOs), inter-governmental organizations, and governments all play different roles in maintaining a peaceful and stable cyberspace. Some countries and regions are further advanced on adopting a multi-stakeholder approach. Speakers mentioned that their organizations are already working to incorporate external actors into their efforts, although establishing trusted public-private partnerships continues to be an issue in some regions. The point was also raised that multi-stakeholder approaches are less likely to take hold in regions where the cybersecurity discussion is driven by defence and intelligence agencies.

[6] See https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf
[7] See https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

As cybercrimes and cyber operations are transnational by nature, effective responses require cooperation to prosecute crimes and address malicious, offensive or aggressive acts. Resource and information sharing between States and between regions can improve the efficiency of law enforcement and attribution. Collaboration and information sharing, specifically sharing of cyber policies or doctrine with others to make intentions clear, were also emphasized as valuable regional CBMs. Lastly, this collaboration can be utilized to promote capacity building. One speaker proposed that regional organizations could create 'cyber assistance teams' that would work with members still developing their capabilities to tackle issues beyond their borders.

Region-specific challenges were also highlighted. For example, in Latin America, public trust in governmental preparedness to handle a major cyber incident is much lower than in many areas of the world. A recent survey indicated that only 16% of Brazilians and 9% of Argentines polled believe that their nations are ready for a major cyber attack compared to 53% of Americans responding to the same poll.[8] Public perception of a government's lack of preparedness and capacity to address cyber incidents corrodes trust in domestic institutions. This "self-interest" argument might be an effective lever to motivate governments to prioritize awareness, policies and initiatives to strengthen cybersecurity.

In South East Asia, a major consideration is its great potential for a boom in the digital economy, particularly through the financial industry. With the rise of breaches and attacks, strategies to mitigate risks need to be adopted now or this economic opportunity could be threatened. Increased efforts in groups like the Asia Pacific Economic Cooperation (APEC) to harmonize approaches to the digital economy among its 21 members would help its members maximize this potential for economic growth.

Promoting cybersecurity and emerging technology industries is a specific priority in the North African region. However, while there is growing, yet uneven, recognition of the importance of artificial intelligence and digitization for economic and social development, the attention of policymakers is often focused on priorities other than cyber or technology issues. Without first securing the buy-in of senior officials as to the importance of cybersecurity policy, investments in capacity-building efforts are unlikely to pay off.

Regional Best Practices and Cooperation

Although multilateral discussions stalled in 2017, regional organizations continued to develop specific activities to further capacity building, agree and implement CBMs, and promote cyber hygiene and best practices in their respective regions. This session explored the variety of approaches regional organizations have employed to operationalize the GGE recommendations in regionally appropriate ways.

One challenge that regional organizations face is that it can be hard to determine who is the national "authority" authorized to engage on cybersecurity issues since many different agencies handle cybersecurity and internal communication and coordination varies. ASEAN placed early emphasis on **building a network of the national actors** responsible for cybersecurity, an investment that ensured that buy in was secured from top-level leadership and laid the foundations for direct engagement on concrete actions.

On **developing regional legislation**, the EU's 2017 Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" [9] contains three main pillars: cyber resilience, deterrence, and international diplomatic engagement. The cyber resilience initiative provides direction on CBMs and information sharing between European States and reformed the European Union Agency for Network and Information Security (ENISA) to better provide training and build capacity among EU members. The

[8] See http://www.pewglobal.org/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/

[9] See https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

deterrence pillar institutes a framework for dissuading potential cyber criminals and malicious actors, including improvements to law enforcement detection, tracing, and prosecution capabilities. The EU also adopted the "cyber diplomacy toolbox" which helps clarify proportionate responses to malicious cyber activities so as to increase EU members' capacity to respond to these actions in a harmonized way. The final pillar, international diplomatic engagement, endorses the norms, rules and principles of responsible State behaviour articulated in the GGE reports. It also establishes guidelines for cybersecurity capacity-building practices intended to increase the level of cybersecurity globally.

A recent illustration of successful **inter-regional cooperation** is based on the experiences of the AU. A questionnaire conducted as part of the AU Convention on Cybersecurity and Personal Data Protection in 2010[10] found that 20% of AU members lacked a cybersecurity strategy, less than 50% had cybersecurity legislation, and approximately only 25% had a Computer Emergency Response Team (CERT). In response, the AU in collaboration with the Council of Europe, Interpol and others organized the First African Forum on Cybercrime in 2018[11] which endeavoured to advance policies and legislation in AU members, foster international cooperation, and build capacity for emergency response. As a priority, they seek to ensure that every member has a national cyber strategy, adopts legislation related to cybersecurity and cybercrime, and creates its own CERT. The main challenges the AU faces in pursuing these goals are the lack of awareness regarding cyber priorities in the national leadership, the lack of participation in global dialogues, and the lack of information about the outcome of these dialogues. A second example is the active collaboration of the OAS with other organizations such as APEC and OSCE, as well as promoting exchanges on best practices with States from outside their region.

In 2016, the OSCE adopted 16 **CBMs** to reduce the risks of conflict stemming from the use of information and communication technologies.[12] The CBMs fall into three main categories: cyber capability sharing, crisis communication mechanisms, and preparedness. These CBMs were referenced repeatedly throughout the workshop as an example for other regional groups to consider following. While some suggested that the objective should be CBMs harmonized at the international level, others argued that regionally agreed CBMs permit the customization of measures that address the particular concerns or challenges of a specific region.

The OAS has developed significant experience with practical awareness and **capacity-building activities**, notably through its mobile simulation lab for cyber response. The cyber lab helps to train incident response personnel throughout the region. Simulation exercises are an effective way to both raise awareness and identify gaps or weaknesses in existing structures, policies or mechanisms that can then be addressed or mitigated.

The importance of **working closely with national cyber "champions"** in each region was illustrated by the support offered by Singapore's Cybersecurity Agency to ASEAN to implement regional initiatives. With the strong leadership of Singapore, in 2017 the ASEAN Ministerial Conference on Cybersecurity formally adopted the existing eleven non-binding norms proposed by the 2015 GGE as part of wider regional stabilization efforts. During its chairmanship of ASEAN in 2018 Singapore prioritized improving coordination and reducing duplication of cyber capacity-building efforts. A second example of a regional champion is the leadership of Japan to establish the ASEAN-Japan Cybersecurity Centre in Bangkok to train regional experts.

[10] See https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[11] See https://au.int/en/newsevents/20181016/first-african-forum-cybercrime
[12] See https://www.osce.org/pc/227281?download=true

An Overview of the GGE and OEWG Processes

In 2018, unable to reach agreement on a single resolution, UN Member States decided to establish both a Group of Governmental Experts[13] and an Open-Ended Working Group[14] to address ICTs and international security. Both resolutions were subjected to a vote, with some States voting in favour of both resolutions.

This will be the sixth GGE established since 2004, and will be comprised of representatives from 25 States, the same number as in 2017. The mandate for the group states that its work will start from the basis of the assessments and recommendations contained in previous GGE reports. As in previous years it will meet behind closed doors, with no observers, and will seek to produce a consensus report. However, unlike previous GGEs, which completed their work within one calendar year, this GGE will start in late 2019 and complete its deliberations in 2021. The GGE will have four sessions (December 2019, March 2020, August 2020, and May 2021) with its report to be submitted to the seventy-sixth session of the General Assembly.

Building on recent precedents, such as the high-level fissile material cut-off treaty (FMCT) expert preparatory group, the GGE resolution provides for two intersessional consultations with the wider UN membership, thereby offering more transparency and inclusivity than the GGE process thus far. The resolution also includes for the first time a consultative process organized in cooperation with regional organizations to share views on issues within the mandate of the group.

The OEWG process is open to all Member States and will work on a consensus basis. The OEWG will start with an organizational meeting in June 2019 followed by three substantive sessions (September 2019, February 2020 and July 2020), with its report to be submitted at the seventy-fifth session. All of the OEWG meetings will occur in New York.

The OEWG's mandate tasks the group to consider further development of specific norms, rules and principles noted in paragraph 1 of the resolution and how to implement them. The mandate also explicitly mentions the possibility of "introducing changes" to those norms or elaborating additional rules of behaviour. The mandate also includes the possibility of intersessional consultations with business, non-governmental organizations and academia.

It cannot be ignored that the unprecedented situation of having two concurrent processes arose from deep divisions about the future of international discussions following the 2017 GGE and thus some fear that the two different forums could compete with or even undermine each other rather than being complementary and mutually reinforcing. By opening up the cyber discussion to all Member States, there is the opportunity to engage the majority of States who have not yet had the opportunity to participate in these issues of global reach and impact. The OEWG will also be the first time international cyber discussions will be held in an open format, which will promote awareness about key issues, lay bare the divisions, and raise the quality of analysis offered by external observers.

[13] A/RES/73/266 of 2 January 2019.
[14] A/RES/73/27 of 11 December 2018.

International Perspectives on Regional Cooperation

While the recommendations contained within the GGE reports are addressed to States, a variety of international organizations are engaged in supporting their operationalization—whether through combatting cybercrime, promoting understanding of how international humanitarian law applies in cyberspace, protecting human rights in the digital environment, or promoting relevant technical standards.

Often international organizations play a leading role in capacity building. For example, the UN Office on Drugs and Crime (UNODC) has taken a regional approach to help States develop cybercrime policies and build the capacity of relevant actors such as law enforcement and criminal justice agencies to gather evidence in transnational cybercrime cases.

Other organizations promote awareness of the principles outlined in the GGE reports. For example, the International Committee of the Red Cross underscores the urgency of adopting shared understandings of how international humanitarian law applies in cyberspace. While the 2013 and 2015 reports state that international law and the principle of sovereign equality applies to cyberspace, in 2017 disagreements over how international law applies contributed to the inability of the group to reach consensus. The EU, for example, has explicitly stated that international law applies in cyberspace. Other regional organizations could make similar declarations as a CBM and transparency measure.

Cybersecurity is a crowded field and all of the panellists in this session identified lack of coordination among the multiple actors—including States, international and regional organizations, sub-regional organizations, and NGOs—as one of the biggest obstacles to progress. They pointed to duplication of capacity-building efforts in some regions, while other regions remain underserved. Many States themselves lack internal coordination on cyber issues, with responsibilities spread across different ministries that do not necessarily collaborate.

As there are many actors within government addressing cyber issues, it is not always evident who is responsible for—or authorized to engage on—matters of international security in the cyber domain. Only a minority of countries have dedicated agencies devoted to cybersecurity; in the rest it can be difficult to identify the relevant officials for discussions. Regional organizations can be essential to overcoming this obstacle by having well-established communication channels throughout governments and the legitimacy to convene any relevant ministry or department.

Issues for International Dialogue

The final session brought together State representatives to discuss how governments can build on the practical measures undertaken by regional organizations during the hiatus of the GGE process to build international agreement.

The new GGE and OEWG are not starting from a blank slate—the previous GGE reports offer a solid foundation to build on and it should not be forgotten that the General Assembly has stated that States should be guided in their behaviour by the recommendations of the 2015 report. There is, however, an urgent need to promote awareness and understanding of the GGE process to-date. Regional organizations are ideally placed to help with this endeavour through renewed efforts to promote understanding of the norms, rules and principles, and capacity-building measures recommended in the previous GGEs.

Cyber specialists within regional organizations have themselves identified the need to have an opportunity to meet with their peers from other regions in order to explore opportunities for inter-organizational cooperation, exchange of information and lessons, and potential informal (or more formal) mechanisms for collaboration. While they often do so on the margins of other meetings, thus far there lacks a structured opportunity in a neutral space for regional organization representatives to discuss specific challenges, exchange ideas and share resources. No one organization is "mandated" to convene the others and attempts to do so thus far have been stymied by politicization by some members.

As more formalized inter-regional Peer to Peer exchanges might not be possible in the current environment, the margins of the OEWG meetings might offer a reoccurring venue for an informal yet regular working-level gathering among peers from regional organizations. Even an informal exchange offers an opportunity to structure and give support to a conversation about their cyber programming and assistance efforts.

Conclusion

It was evident from the day's discussions that regional organizations are essential partners in building a stable and secure cyber environment for all States. While international discussions tend to focus on seeking agreement on higher level principles, regional organizations have taken the lead in "translating" these into concrete actions.

Regional organizations should also be recognized as indispensable partners in the eventual success of the GGE and OEWG processes. Building on their existing activities at the regional level to raise awareness, build capacity, foster dialogue and enhance trust, regional organizations will be essential to creating a community of experts who can engage in the international discussions.

The Role of Regional Organizations in Strengthening Cybersecurity and Stability: Experiences and Opportunities

Report of the 2nd International Security Cyber Workshop Series
Geneva, Switzerland, 24 January 2019

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 third in the series, brought together representatives from regional organizations, 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