Regional Consultations series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

Overview

Mandate

In December 2018, the General Assembly of the United Nations established a Group of Governmental Experts (GGE) pursuant to resolution 73/266, entitled "Advancing responsible State behaviour in cyberspace in the context of international security."

By the same resolution, the General Assembly requested the Office for Disarmament Affairs of the Secretariat to collaborate with relevant regional organizations to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions.

Modalities

To undertake this request, the UN Office for Disarmament Affairs is organizing a series of consultations between members of the GGE and Member States of the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe, the Regional Forum of the Association of Southeast Asian Nations and the League of Arab States.

The 6 separate consultations will be 1-2 days in duration and organized in the period of 2019-2020 in cooperation with the respective regional organizations. To the extent possible, the consultations are intended to take place in conjunction with existing meetings of the regional organizations related to international ICT-security.

While each of the regional consultations would be tailored to the priorities of each region, in general terms, the consultations will include: 1) presentations on the work of previous GGEs; 2) free-flowing discussions between participating GGE members and the member States of the respective regional organizations; and 3) wider multi-stakeholder consultations, engaging civil society, private sector and academia where agreed.

Objectives

The regional consultations provide a unique opportunity to enrich the GGE process with regional perspectives on questions pertaining to ICT and international security, and to exchange views on the experiences of regional organizations and their member States on measures and policies

aimed at further promoting a peaceful and secure global a peaceful regional and global ICT environment.

At the same time, the regional consultations are designed to promote further awareness of the work of the GGEs. They also constitute a response to the call by many UN Member States for enhanced inclusiveness in the GGE process on the issue of cybersecurity, which impacts all States. The exchange between GGE members and member States of regional organizations can also promote complementarities between the work of GGE and the OEWG.

Participation

The GGE Chair, Ambassador Guilherme Patriota of Brazil, or a GGE member designated by the Chair to attend on his behalf, will attend all regional consultations. All other GGE experts are cordially invited to participate in the consultations with the regional organizations of which their government is a member State. The regional consultations will be supported by the UN Office for Disarmament Affairs (UNODA), the UN Institute for Disarmament Research (UNIDIR) and experts, including previous GGE consultants, who will provide an overview of the GGEs to date.

Presentations on the work of the previous GGEs

Expert consultants to the previous GGEs, Dr. James Lewis, Senior Vice President at the Center for Strategic and International Studies (CSIS), and Dr. Camino Kavanagh, Visiting Fellow, Department of War Studies, King's College London, provided an in-depth overview of the work and recommendations of previous GGEs ahead of each of the consultations, the main elements of which are captured in the following.

Historical overview

The issue of ICT security has been on the UN agenda since 1998, when the Russian Federation introduced a draft resolution on the subject in the First Committee of the UN General Assembly. It was then adopted without a vote by the General Assembly as resolution 53/70.

Since 2004, five Groups of Governmental Experts (GGE) have continued to study the threats posed by the use of ICTs in the context of international security and how these threats should be addressed. Three of these Groups have agreed on substantive reports with conclusions and recommendations that have been welcomed by all UN Member States. Furthermore, each GGE built on the work done by the previous one, making significant cumulative progress on the issues at hand.

The GGE reports have been well-received by the General Assembly of the United Nations. In particular, the 2015 report of the GGE was adopted by consensus in resolution 70/237. This resolution "calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts."

Cumulative nature of the GGE reports

The GGE reports should be viewed as cumulatively developing a normative framework for States in their use of ICTs over time.

The 2010 GGE envisaged the discussion of voluntary norms, rules and principles of responsible State behaviour, Confidence-Building Measures (CBMs), and capacity-building in the use of ICTs in the context of international security.

The 2013 GGE report embeds cybersecurity in the existing structure of international relations. It highlights the centrality of the UN Charter, State sovereignty, international law, and created a general framework for state responsibilities and for cooperation.

The 2015 GGE report reiterated and expanded on the recommendations of the 2013 GGE report and further defined voluntary norms and confidence-building measures.

It recommended 11 voluntary, non-binding norms of responsible State behaviour, which cover a range of issues, including cooperation between States in developing and applying measures to increase stability and security in the use of ICTs; respect for human rights in the use of ICTs; protection of Critical Infrastructure; and that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

The 2015 GGE report also identified a number of CBMs aimed at expanding transparency and improving cooperation. It reaffirmed the assessment of the 2013 GGE report that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT-environment. It also laid out State responsibilities under existing international law.

Most recent GGE of 2016-2017

In accordance with its mandate, as contained in resolution 70/237, the 2016-2017 GGE undertook a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international security. Furthermore, the Group took into account the reports of the previous GGEs, as well as contributions and proposals made available by members of the Group. Several draft substantive reports were considered by

the Group on existing and emerging threats; capacity-building; confidence-building; recommendations on the implementation of norms, rules and principles for the responsible behaviour of States; application of international law to the use of information and communications technologies; and conclusions and recommendations for future work. However, no consensus was reached on a final report.

Summary of Consultations with participating States of the Organization for Security and Cooperation in Europe 17-18 June 2019, Bratislava

The 17-18 June 2019 GGE consultations with OSCE participating States took place during the annual OSCE cyber conference, entitled "Cyber/ICT Security for a safer future: The OSCE's role in fostering regional cyber stability", which was opened by Ambassador Radomír Boháč of Slovakia, Chairperson of the OSCE Permanent Council Permanent Representative of the Slovak Republic to the OSCE. The GGE consultations were organized by the OSCE Secretariat's Transnational Threats Department (TNTD), in collaboration with UNODA.

The GGE consultations were facilitated by Ambassador Károly Dán, Permanent Representative of Hungary to the United Nations (Vienna), and Permanent Representative to the Organization for Security and Co-operation in Europe and other International Organizations in Vienna, in his capacity as Chair of the Informal Working Group (IWG) established by PC decision 1039, and Ambassador Guilherme de Aguiar Patriota, Chair of the 2019/21 UN Group of Governmental Experts. Ambassador Jürg Lauber, Chair of the Open-ended Working Group, also provided a brief statement.

The closed session was preceded by a briefing and interactive discussion about previous GGE meetings and reports titled "Multilateral cyber diplomacy: a discussion on UN processes around cyber/ICT", presented by Dr. James Lewis, Senior Vice President at the Center for Strategic and International Studies (CSIS), and Dr. Camino Kavanagh, Visiting Fellow, Department of War Studies, King's College London.

Exchange of views on confidence building measures

The Organization for Security and Co-operation in Europe, since 2013, has developed 16 pioneering Confidence Building Measures (CBMs) to reduce the risks of conflict stemming from cyber/ICT activities. The implementation of these CBMs is a key priority of the OSCE's 57 participating States. This was most recently reaffirmed at the OSCE's Ministerial Council in 2017. An Informal Working Group continues to drive co-operation forward, including through its flagship "Adopt a CBM" initiative. A key focus of the GGE consultations with the OSCE was therefore to exchange views, ideas and lessons learned with the OSCE on the development and implementation of CBMs with a view to taking forward the work of the GGE.

OSCE participating States reflected on the threat posed by the use of ICTs which some saw as a "cyber tsunami", undermining trust between States. It was stressed that there needs to be an

emphasis on advancing responsible State behavior through agreed norms and common understanding of issues and challenges rather than just focusing on the technology itself.

It was noted that CBMs do not work in a vacuum. Rather, these measures require existing trust and cooperation between States. Such trust could be developed in any number of ways, including in areas and fields of work other than the one in question.

It was highlighted that communication is central to CBMs, and technical issues, such as regular communications checks and updating list of points of contact, was vital to achieving effective communication flow.

A central point raised was that States' ability to implement transnational CBMs is closely linked to national capacity. Transparency measures such as sharing cyber doctrines and national cyber strategies, imply a requisite capacity for internal coordination and the means to develop and adopt such policies.

Given the transborder and global nature of ICT threats, it was also stressed that CBMs need to be made more interoperable between regions by connecting various hubs around the world. The GGE and OEWG could potentially play a key role in fully universalizing information exchange procedures and other CBMs.

The experience of OSCE in undertaking consultations on the adoption of CBMs was also underscored as potentially useful for consideration by the GGE. Steps that enabled agreement included encouraging open and inclusive debate and a phased approach, starting with low-hanging fruit, on what can be agreed; and an emphasis on taking the necessary steps to ensure the implementation of the CBMs.

The GGE Chair noted that CBMs in the GGE process could be seen as a wider system of information sharing and capacity building rather than just isolated measures, and that there should be an ongoing interaction with regional organizations such as the OSCE so that States can continue, at the regional level, to feed into the GGE process as it proceeds.

Taking forward the GGE and OEWG processes

The GGE Chair and members and OSCE participating States placed particular emphasis on exchanging views on how to take forward the GGE and OEWG processes.

OSCE States expressed support for both processes and viewed that the participation of the Chairs of both processes at these regional consultations was a positive sign of cooperation.

Several ways were proposed for dividing the work between the OEWG and GGE, with suggestions for both groups to potentially focus on different issues but with mutually-reinforcing results. It was also highlighted that there should be an optimal use of the limited time available for the work of both groups.

States also reaffirmed the legitimacy of both the GGE and OEWG processes as having been mandated in resolutions adopted by the UN General Assembly.[1]

It was emphasized that the previous GGE reports had enjoyed GA endorsement, particularly in GA resolution 70/237, in which Member States were called upon to be guided in their use of ICTs by the 2015 GGE report.

Participants stressed that the 2015 GGE report provides a pathway on how to set out the work, and that the reopening of previously agreed elements of the GGE reports should be avoided.

It was also highlighted that efforts needed to be made to ensure that the GGE processes become better known in the international community and to encourage the implementation and universalization of previous GGE recommendations.

OSCE States noted that the GGE and OEWG are complementary, but that there is a degree of overlap in the mandates. They appreciated the inclusive outreach of the GGE process, noting that the OEWG provides an opportunity for countries that have been less engaged on the issue of ICT-security in the context of international security to join the conversation.

Several perspectives were provided on the substantive issues under the GGE's mandate, noting that in considering the applicability of international law in the use of ICTs, the Tallinn Manual provides an academic perspective, but more work would be needed.

[1] GA resolution 73/27 established the OEWG and GA resolution 73/266 requested the UN Secretary-General to establish the GGE.

Also on the issue of international law, some States suggested the need to look into the legal concept of due diligence, particularly where actions within one State's territory affect the rights of other States.

Some OSCE States also noted the need to protect the rights of individuals from the impact of cyber operations, including where such operations impact critical infrastructure. In this regard, cooperation between States and civil society is indispensable, and further effort is required to ensure that all members of the global community can attain a higher cyber capacity.

Multi-stakeholder engagement at the OSCE regional consultations

A central aim of the regional consultations was to also engage with private sector, civil society and academia on the work of the GGE.

A multi-stakeholder session of the consultations entitled "Global Advancements and Regional Efforts: Addressing International Cyber/ICT security policy challenges" was held immediately after the closed consultations with OSCE participating States. Ms. Izumi Nakamitsu, UN Under-Secretary-General and High Representative for Disarmament Affairs, gave a keynote speech encouraging deeper regional engagement between the GGE and States at the regional level. A panel discussion, moderated by Ms. Rasa Ostrauskaite, Director, Transnational Threats Department, OSCE Secretariat, followed, with participation by Ambassador Guilherme Patriota, Ambassador Jürg Lauber and Ambassador Károly Dán.

Non-governmental Organizations attending the meeting raised a number of concerns and questions about how international human rights issues would be reflected in the GGE and OEWG processes. While human rights issues are central to the use of ICTs, as acknowledged and reaffirmed in the voluntary, non-binding norms of responsible State behaviour recommended in the 2015 GGE report,[2] the focus of the GGE is also on the peace and security aspects of the use of ICTs.

[2] Norm (e) of the 2015 GGE report states the following @States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;" (A/70/174)

Summary of Discussions by the Chair of the GGE

At the end of the consultations, the GGE Chair summed up the discussions, noting that participants had:

- Highlighted the importance of ensuring complementarity between the GGE and the OEWG through i) the work of the respective Chairs and Member States; and ii) having the same Secretariat and technical team supporting both processes.
- Demonstrated broad agreement that the new processes should build on the outcome of previous GGEs, and that all effort should be made to avoid fragmentation and duplication between the two processes, as well as reopening or undermining agreed understandings reached in the previous GGEs.

- Stressed that the 2019-2021 GGE should provide value by building on the work of the previous GGEs when addressing the issues in its mandate. Furthermore, that the GGE mandate has a particular focus on international law and allows for the annexing of views on this issue, which would enrich the GGE outcome.

- Identified that exchanges between the GGE and OSCE should be ongoing. The OSCE experience on CBMs is advanced. These experiences – as well as others on capacity building – can inform the GGE. It will be equally important to learn from other regional experiences through involving other actors engaged in this field, including from the private sector, non-governmental organizations and academia.

Summary of Consultations with European Union member States
19-20 June, Brussels

The Consultations with European Union member States were held from 19-20 June, within the context of the EU Horizontal Working Party on Cyber Issues (HWP). The HWP was established in 2016 and is responsible for coordination of the European Council's work on cyber issues, supported by the European External Action Service (EEAS).

As with the regional consultations with OSCE participating States, consultations with EU member States comprised three components, including an overview of the work of the previous GGEs, presented by presented by Dr. James Lewis, Senior Vice President at the Center for Strategic and International Studies (CSIS), and Dr. Camino Kavanagh, Visiting Fellow, Department of War Studies, King's College London; a closed session between EU member States and the GGE Chair and GGE members, facilitated by Mr. Rory Domm, Head of the Security Policy Unit, EEAS; and wider consultations with civil society.

Some participants indicated that holding the consultations with EU immediately after the consultations with OSCE participating States was a good continuation of discussions given the significant overlap of membership between the two regional organizations.

Exchange between GGE Chair and members and EU member States

In terms of existing and potential threats, participants emphasized the need to highlight the opportunity cost of not having a functioning global internet and the increasing instability in cyberspace. In this regard, the work of the GGE should not be disconnected from other UN issues such as the Sustainable Development Goals.

Participants also noted that that lower level ICT-threats could potentially be more worrisome as they could be more tempting for some to carry out these operations. It was suggested that interference in democratic processes through cyber means should not be excluded from the discussion, given its potential impact on peace and security.

It was stressed that a profound regard for rights was required to ensure a stable and peaceful cyberspace, and that this should not be reduced to a discussion on balancing values with security. In considering how international law applies to the use of ICTs, an emphasis should be placed on

a human-centric approach to cybersecurity, which might also include issues related to gender and broad participation.

A common theme raised during the discussions was the need for greater awareness-raising and capacity-building of States not only at the national level, but also in relation to the capacities required to engage in multilateral negotiations on cyber issues.

On the issue relating to norms of responsible State behavior, participants stressed that norms agreed in previous GGEs should not be revisited and that progress be made on questions relating to their implementation. It was also noted that new norms could potentially be discussed. For instance, reference was made to the norms proposed by the Global Commission on the Stability of Cyberspace, such as the norm to protect the public core of the internet, as well as the recommendations of the Paris Call for Trust and Security in Cyberspace.

Another suggestion related to the establishment of a global repository of existing practice within the United Nations. This could enable any UN Member State to showcase how it is implementing the voluntary norms of responsible State behavior, confidence building and other measures recommended by previous GGEs. In this regard, lessons might be derived from the Dinard Declaration on the Cyber Norm Initiative adopted by G7 countries in April 2019, which aims to encourage voluntary exchange of information, best practices, and lessons learned on implementation of voluntary, non-binding norms of responsible State behavior.

Emphasis was placed on the point that confidence-building measures should not only be discussed in and of themselves. They can also serve important political functions, integral to formulating a common stability framework for cyberspace. Some also pointed to the EU Cyber Diplomacy Toolbox as a useful precedent.

On international law, some raised the possibility of developing an overarching statement on the issue. A question was also put forward on the role of the United Nations Security Council regarding cyber/ICT-issues and international peace and security.

Participants discussed the moderating role of the EU in intergovernmental processes, that it should act as a force for good in the world and in the promotion of a rules-based and human rights-based cyberspace. The EU could also play a lead role in discussions related to the protection of privacy of data and undue intervention on democratic institutions.

At the same time, it was emphasized that the issue of rights and security should not be considered as mutually exclusive, since one cannot exist without the other. Participants also stressed that there is a need to determine where consensus can be found without rolling back the gains of past GGEs.

Multi-stakeholder engagement at the EU consultations

On 20 June, consultations were conducted between GGE members from the EU, EU member States and members of civil society. The meeting was organized by the European Union Institute for Security Studies (EUISS). The consultations were Chaired by Ambassador Guilherme Patriota and facilitated by Mr. Gustav Lindstrom, Director, EU Institute for Security Studies; Mr. Patryk Pawlak, Brussels Executive Officer and Project Coordinator for the EU Cyber Direct, EUISS; and Mr. Wiktor Staniecki, Security Policy Unit, EEAS.

Participants discussed the need for a resilient digital society grounded in rights and a rules-based international order to be achieved through two possible paths, a state-centric and a civil society-centric pathway.

For States, there needs to be cooperation through multilateral processes and laws. Meanwhile, a civil society pathway would represent a more robust and inclusive space where cybersecurity is a shared responsibility. It was suggested that the EU needs to redirect its approach to steering change and better communicate the value of the EU's normative agenda, including through leading by example.

Participating think-tank and civil society representatives emphasized the need to democratize the debate within the GGE through the involvement of regional organizations, CSO-led initiatives, as well as other UN agencies and committees. They also stressed that given the nature of ICTs, it is necessary not only to seek the views of civil society and the private sector in particular, but also to obtain their buy-in. In order to achieve this, the interests of civil society and the private sector needed to be clearly formulated and transmitted to the GGE so that they can be considered and reflected in agreements accordingly.

Participating civil society organizations also discussed ways in which the outcomes of the GGEs could be disseminated with the goal of raising all Member States capabilities and resources for developing and implementing recommended policies. Some highlighted that countries from

around the world will participate on an equal footing in the intergovernmental processes and the focus should be on cooperative capacity building that advances responsible State behavior in cyberspace.

Summary of Discussions by the Chair of the GGE

The GGE Chair summarized the key points raised during the meeting, including the following:

- There was a need to develop a work programme for the GGE which could be issue-based while still responding to the mandate.

- The EU and its member States have a key role to play in building bridges between countries and positions.

- The EU and its member States could also provide contributions on issues where there could be agreement across countries, including on privacy and data protection.

- There already seemed to be broad agreement that "we should not undo what has been done", with an understanding that there should be no fragmentation, no regression and no rolling back.

- Confidence building measures should not be construed as superficial measures but as a system or a framework for providing information and assistance. They could be seen as a buffer against threats and a mechanism for coordinating responses to threats, a form of preventive and reactive diplomacy.

- Succinct contributions from civil society were encouraged via contributions channeled through EU member States represented on the GGE or through inputs from the EU as such for the consideration of GGE members. Technical issues could be better translated into the GGE report, with input from NGOs.

- There should be an ongoing exchange with regional organizations, in which contributions to the GGE could continue in a dynamic manner.

Summary of Consultations with member States of the Organization of American States (OAS) 15-16 August 2019, Washington D.C.

The Regional Consultations with OAS member States were held from 15-16 August, within the context of a meeting of the Inter-American Committee against Terrorism (CICTE), and with the support of the CICTE Secretariat.

These consultations comprised three components, including an overview of the work of the previous GGEs; an open and inclusive multistakeholder session; and a session between OAS member States and the GGE Chair and GGE members, facilitated by Mr. Michael Walma of Canada, Member of the 2013 and 2017 Groups of Governmental Experts.

The first day of the consultations was opened by Mr. François Jubinville, Interim Representative of Canada to the OAS, Chair of CICTE, Mr. Patricio Aguirre Vacchieri, Representative of Chile, Chair of the OAS Working Group on Cooperation and Confidence-Building Measures in Cyberspace and Ms. Alison August Treppel, Executive Secretary, CICTE.

Multistakeholder engagement at the OAS regional consultations

Participants stressed that the multistakeholder approach is the only approach, since in an interconnected world, we are only as strong as our weakest link. Furthermore, private corporations have demonstrated readiness to engage with States in this area as most recently evidenced by its support for the November 2018 Paris call for trust and security in cyberspace and its nine principles, which draw from previous GGE recommendations.

It was proposed that the private sector could support States in the following additional areas:

- Sharing threat intelligence for incident prevention and response.
- Sharing information and research on malicious actors.
- The provision of legal expertise that could be drawn upon in terms of discussions on how international law applies in the use of ICTs.

Civil society experts called on Governments to provide assistance to those impacted by cyber incidents and to more concretely operationalize norms, including those on the protection of critical infrastructure.

It was also stressed that the voices of civil society should be better heard at both the GGE and the OEWG processes, and that these processes should be made more transparent.

Participants emphasized that the public and private sectors needed to move together towards supporting the observance of norms and that spaces needed to be created for such collaboration. Some participants also expressed concern at the fragmented approaches in addressing cyber security, where there is a multitude of events and initiatives without much clarity on how various actors could participate.

The Role of Regional Organizations in relation to the GGE and OEWG processes

This issue was discussed in-depth during the first day of the consultations. The following points were highlighted:

- Regional bodies can improve understanding, pursue capacity building as well as amplify and aggregate voices that need to be heard.
- Regional bodies are also more agile and fast-moving than at the global level.
- Regional organizations can have a brief-back role where they can report to countries who weren't at the GGE ensuring better information-sharing.
- The regional organizations can help with awareness-raising on the work of the GGEs.
- A networking function was potentially available at the regional level for working across regions.

Participants noted that OAS was an excellent platform for discussing cyber issues given its track record in finding common ground between diverse views between states. Furthermore, through its Working Group on Cooperation and Confidence-Building Measures in Cyberspace, OAS has already agreed to develop six measures to enhance cooperation and confidence across the region and is developing detailed guidance on how to implement a number of these measures.

Exchange of views between OAS Member States and the GGE Chair and members

The consultations with OAS member States held on Friday 16 August were opened by Ms. Izumi Nakamitsu, UN Under-Secretary-General and High Representative for Disarmament Affairs and the Chair of the GGE, Ambassador Guilherme Patriota of Brazil. The Chair of the Open-ended Working Group, Ambassador Jürg Lauber of Switzerland, also made brief opening remarks.

Expert consultants to the previous GGEs, Dr. James Lewis, Senior Vice President at the Center for Strategic and International Studies (CSIS), and Dr. Camino Kavanagh, Visiting Fellow, Department

of War Studies, King's College London, provided an in-depth overview of the work and recommendations of previous GGEs.

Participants highlighted that the threats from cyberspace are transnational in nature. Threats do not have to emanate from a country or region for its impact to be felt there. Thus every State should be encouraged to formulate their views on these issues.

States expressed their confidence and trust in both the GGE and OEWG Chairs and welcomed the open channels between the two Chairs to ensure harmonization between the two processes.

Participants reaffirmed that, as agreed in the 2013 and 2015 GGE reports, international law is applicable in cyberspace, including the UN Charter in its entirety. Participants stressed also the applicability of international human rights law, international criminal law, customary international law and international humanitarian law in this space. It was highlighted that respect for international law also guarantees the sovereignty of States in cyberspace.

It was noted that the topic of how international law applies in the use of ICTs should be addressed from an affirming perspective. In this regard, the work being done by the inter-American Juridical Committee (CJI) of the Organization of American States to compile and publicize OAS member States views on the application of international law to cyber operations would be an important contribution to on-going discussions.

Participants recalled that previous GGE reports recommended 11 voluntary non-binding norms of responsible State behaviour, as well as concrete measures for confidence-building (CBMs) and capacity-building. Furthermore, UN General Assembly in resolution 70/237 called upon Member States to be guided in their use of information and communications technologies by the GGE 2015 report.

The importance of confidence building measures and their strong linkage to mutual cooperation and the preservation of peace in cyberspace was emphasized. States highlighted that in order to strengthen confidence building among States, additional measures were needed such as: 1) the designation of points of contact particularly in foreign affairs ministries; 2) the strengthening capabilities through seminars and workshops; 3) the provision of basic training courses for diplomats and other national officials; 4) the fostering of best practice exchange; and 5) sharing of information on national policies, strategies and legislation.

While noting the focus of GGE and OEWG discussions will be on international security, participants stressed that the related issues of human rights, security, crime and development in the cyber context should not be discussed within silos, rather, there should be better interaction between these topics.

It was noted that the previous GGE reports provide limited guidance on how to implement norms and CBMs and other measures. The work of the new GGE could focus on developing a roadmap of implementation guidance on measures and norms already agreed to rather than focus on the development of new norms.

In this regard, participants stressed that the GGE should have its starting point the agreements from previous GGEs. They also noted the that the sharing of views on how States believed international law applies in cyberspace, as foreseen in the GGE's mandate, would contribute to better transparency and an environment of mutual understanding.

It was also proposed that OAS should establish a working group to convene quarterly discussions on the use of ICTs in the context of international security, including on the implementation of agreed measures including CBMs, with a view to fully participate in UN processes.

Summary of Discussions by the Chair of the GGE

At the end of the consultations, the GGE Chair summed up the discussions, noting that participants had:

- Indicated that the work of the GGE comes under the First Committee of the UN General Assembly and should therefore remain its focus on international peace and security concerns.
- Stressed the importance of not accepting any backward movement to what has been agreed, which should be considered sacrosanct.
- Expressed deep support for multilateralism and for both the GGE and OEWG processes, as well as a wish for these processes to succeed. Such success could include

1. Constructive and useful discussions within the GGE that increase overall understanding of the issues that lie ahead;
2. Picking up on and taking forward points of commonality;
3. Establishing a better understanding and implementation of norms and principles and CBMs in the use of ICTs;
4. Developing a framework for cyber security based on confidence and capacity-building measures along with cooperative steps to monitor and respond to cyber threats.

The GGE Chair also highlighted that:

- Different regions have different priorities and interests. OAS has a significant *acquis* when it comes to international law and it is undoubtedly in a position to contribute

constructively to GGE discussions on how international law applies to State use of ICT. The OAS CJI initiative will be an important contribution in this regard.

- The OAS is well-placed to study the GGE-recommended norms and CBMs more systematically, identifying the structures, mechanisms and resources that need to be put in place nationally to support their implementation.

- The OAS can serve as a platform for receiving input from non-governmental organizations and private sector entities, and to channel these into its own discussions and contributions to the GGE process.
- The OAS should continue to mobilize in support of the GGE, and to keep an open channel for ongoing dialogue. Written contributions from OAS and its members to the GGE were encouraged.

Summary of the Regional Consultations between member States of the African Union and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
11 October 2019, African Union Headquarters

Overview

The Regional consultations with member States of the African Union and representatives of the African Union Commission were organized within the context of the "Addis Ababa Cyberweek" in coordination with the Chatham House, the Global Forum on Cyber Expertise (GFC) as well as the Global Commission on the Stability of Cyberspace (GCSC).

First, the GGE process was discussed at a Chatham House event for Commonwealth Countries on 7 October. Afterwards, a historical overview of the GGE process was provided by the UNIDIR support team during the GFCE round-table discussion on 9 October. Then, the GGE Chair and the Chair of the Open-ended Working Group interacted with the GFCE "Group A task force on norms, CBMs and cyber diplomacy" on 10 October.

Broad discussions were held in the morning of 11 October by a joint event between the GCSC, GFCE, and the UN GGE.

The actual regional consultations between member States of the African Union and the Group of Governmental Experts were held at the African Union Commission Headquarters in the afternoon of 11 October and were attended by government representatives of AU Member States, representatives of the AU Commission, as well as by some representatives of non-governmental organizations, private sector companies and academia.

Multi-stakeholder exchange of views between the GGE Chair, members of the AU, the GSCS, the GFCE and non-governmental stakeholders

Brief presentations were made by the Chair of the GGE, Ambassador Guilherme Patriota; the Chair of the Open-ended Working Group, Ambassador Jürg Lauber; Co-Chairs of the GCSC, Mr. Michael Chertoff, Co-founder and Executive Chairman at the Chertoff Group, and Ambassador Latha Reddy, former Deputy National Security Adviser of India; Dr. James Lewis, Senior Vice President at the Center for Strategic and International Studies (CSIS); and Mr. Chris Painter, GCSC Commissioner and Chair of the Global Forum for Cyber Expertise Working Group on Strategy and Policy. The meeting was moderated by Mr. Moctar Yedaly, Head of Information Society Division,

African Union Commission.

The Global Commissioners recalled the mandate under which they work to "develop proposals for norms and policies to enhance international security and stability" of the cyberspace, building upon the norms agreed in the 2015 UNGGE report. They then presented key sections of the Commission's forthcoming final report (Advancing Cybersecurity, of November 2019), explaining the rationale and clarifying recommendations for a framework for the stability of cyberspace, encompassing six principles described as: responsibility, restraint, duty to act, human rights, adherence and accountability. They emphasized the endorsement by the Commission of a norm to protect the public core of the Internet and another norm to protect the technical infrastructure essential to elections, referenda or plebiscites. They presented the set of norms recommended in the report, as follows:

1. State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

2. State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

6. Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7.States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

During discussions, some participants referred to the possibility of developing a general norm, mechanism or system dedicated to capacity-building for the implementation of principles and norms, while others were of the view that capacity-building should take the form of special programs tailored to specific needs and priorities. Many highlighted the cross-cutting nature of capacity-building.

Participants raised the importance of ensuring that norms reflected not only the responsibility of States but also of non-State actors such as private sector companies.

It was suggested that in carrying out their mandate, the GGE and OEWG needed bear in mind broader cyber challenges including cybercrime, terrorist use of the internet as well as development, with the Sustainable Development Goals providing useful guidelines and harmonizing principles.

Some expressed the view that while the GGE and Open-ended Working Group implement mandates related to the behavior of States, the GCSC has also focused on and made recommendations for non-state actors in a manner that further extends and complements the scope of GGE and OEWG considerations.

It was proposed that aspects of the GCSC's report of relevance to the GGE's mandate could be used as an important input for the GGE discussions, including recommendations on principles, norms and regulations.

Discussions addressed how to obtain contributions from non-governmental organizations (private sector, academia, civil society) as part of the UN intergovernmental processes. It was suggested that States could bring to the attention of the GGE and the Open-ended Working Group key initiatives and ideas emanating from other relevant fora.

Some participants pointed out that the international community is at a turning point on how cyberspace and cybersecurity are perceived and dealt with, and that traditional modes of action may no longer be sufficient to meet the challenges posed by the digital medium. It was suggested that the work output of dedicated entities such as the GCSC, GFCE and the Conference on cybersecurity, among other efforts, can contribute significantly to a framework on cybersecurity.

Exchange of views between the GGE Chair, member States of the African Union and representatives of the AU Commission

Consultations between the GGE Chair, other members of the GGE, representatives of member States of the African Union and of the AU Commission were chaired by Dr. Katherine Getao, CEO, ICT Authority, Kenya, a member of the GGE herself. Mr. Adil Sulieman, Senior Policy Officer, Telecom and ICT, of the African Union Commission delivered welcoming remarks, and both the GGE Chair as well as the Chair of the Open-ended Working Group followed with opening statements of their own. A historical overview of the work of the GGEs was presented by Ms. Kerstin Vignard and Dr. Camino Kavanagh from the UNIDIR support team to the GGE and OEWG processes.

Substantive discussions focused on two key topics, namely, what the African priorities on cybersecurity were and how these could be reflected in the UN GGE's work, as well as how the recommendations of the UN GGEs were being implemented in the region.

Dr. Albert Antwi-Boasiako, National Cybersecurity Advisor, Ministry of Communications, Ghana; Mr. Abdul-Hakeem Ajijola, Executive Chairman, Consultancy Support Services Ltd and Member of the Organization of the Islamic Cooperation – Computer Emergency Response Team (OIC-CERT); and Ms. Anriette Esterhuysen, Senior advisor on internet governance, policy advocacy and strategic planning, Association for Progressive Communications (APC), made presentations to kick-off the substantive discussions. Lead Statements from the floor were also made by the following previous and current GGE members from the region, followed by an interactive discussion among all participants:

- Dr. Chérif Diallo, Director of Information and Communication Technologies (ICT), Ministry of Digital Economy and Telecommunications, Senegal
- Advocate Doctor Mashabane, Chief-Director: United Nations, South Africa
- Mr. Hassan Mokhlis, Director of ICT, MFA, Morocco
- Mr. Kaleem Usmani, Officer-In-Charge, CERT-MU, Mauritius

Discussants emphasized the rapidly expanding use of internet and social media in Africa. It was stressed, however, that greater political effort and will were necessary for engaging countries of the region in international ICT-related processes, through awareness raising regarding the urgency of these issues at the highest political levels.

It was suggested that the African region could develop coordinated positions and contributions not only on capacity building requirements and delivery, but equally on the substantive discussions about principles, norms and regulations for the responsible behavior of States in cyberspace in the context of international peace and security. Collaboration between previous and current GGE members designated by African countries could be explored in these efforts.

The African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014, was highlighted as an important regional initiative for the GGE, which more States should be informed of.

African countries in their efforts to address cybersecurity could be guided by the 2015 GGE recommended norms in a more concrete manner, and a culture of collaboration for the peace and stability of cyberspace within the framework of the African Union could be fostered to encourage implementation of these norms.

Particular emphasis was placed on the need for all countries to respect human rights in the use of ICTs as set out in norm (e) of the voluntary, non-binding norms of responsible State behaviour of the 2015 GGE report.[3] Gaps in in this respect needed to be assessed and identified, and cooperation for capacity building strengthened in support of greater adherence to applicable norms.

Some recommendations on capacity building were aimed at putting in place or improving national institutional frameworks for cybersecurity, including the development of national cybersecurity policies and strategies. The need for increased collaboration between relevant national entities at the ministerial level was underscored.

Emphasis was placed on the urgency of protecting critical infrastructure from cyber-attacks, including through the development of critical information infrastructure protection plans.

It was noted that trust between states is essential for cooperation to take place in a range of sensitive but important areas, from the harmonization of legislation on cybersecurity and cybercrime to information sharing and incident reporting.

The importance of putting in place sustainable financing facilities or mechanisms in support of national cybersecurity efforts was underscored. The African Union Commission was named an important resource for states of the region on the issue of cybersecurity.

Summary of Discussions by the Chair of the GGE

At the end of the consultations, the GGE Chair:

- Welcomed the African Union's determination to deepen engagement with and provide inputs to the ongoing United Nations GGE and OEWG processes.

[3] This norm sets out the following: "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;" (2015 GGE report, A/70/174)

- Recognized the wider implications of cybersecurity but underlined that the work of the GGE focuses on international peace and security concerns within the context of the UNGA 1st Committee, and contributions should be formulated accordingly.
- Expressed the view that enhanced cooperative actions, including the harmonization of national laws on cybersecurity through non-binding voluntary principles, norms and regulations should nevertheless occur in alignment with universally endorsed recommendations and commitments. And these needs to constantly evolve through a gradual buildup of additional layers of common understandings and consensus at the multilateral, regional and national levels.
- Observed that several aspects of the work carried out by the GCSC and the GFCE, as presented and discussed in Addis Ababa, seemed directly relevant to the GGE and would greatly benefit discussions and progress if taken into account.
- Underscored that widespread adherence to norms of responsible State behavior was central and that improved capacities were required to level the playing field among different countries and regions in this respect.

The GGE Chair also:

- Encouraged regions to clearly formulate and express their respective priorities and interests regarding cybersecurity in the context of international peace and security by providing clear, synthetic inputs to the GGE in written or other forms.
- Called upon the African Union to put forth coordinated positions on all issues to be discussed in the current GGE, departing from the adopted 2015 GGE report.
- Believed such contributions would promote compliance with the regional dimension embedded in resolution 73/266, and should be provided in an evolving and continuous basis through the good offices of the Chair and the African Union's Commission.
- Noted capacity building for cybersecurity can be construed as an articulated system of cooperation and support for the implementation of norms and recommendations emanating from the ongoing UN processes; but should not be pursued merely for the sake of having an outcome in the face of difficulties in other areas of agreement also under consideration. The GGE should aim for an a balanced, cohesive and comprehensive outcome, reflecting the concerns and interest of a wide range of members and stakeholders.
- Suggested strengthened norms, transparency and confidence building measures, institutional arrangements for dialogue and implementation, together with a more robust capacity building delivery system could help consolidate a framework for advancing responsible behavior in cyberspace in the context or international peace and security.

Summary of the Regional Consultations between member States of the Association of Southeast Asian Nations and its dialogue partners and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security

2 October 2019, Singapore

Overview

The Regional consultations between member States of the Association of Southeast Asian Nations and its dialogue partners and the Group of Governmental Experts took place within the context of the 4th ASEAN Ministerial Conference on Cybersecurity (AMCC) convened in Singapore on 2 October 2019.

The AMCC was chaired by Mr S. Iswaran, Minister for Communications and Information and Minister-in-Charge of Cybersecurity of the Republic of Singapore. The GGE Chair and the Chair of the Open-ended Working Group (OEWG) attended these consultations. The Chairs of both processes also held interactive multi-stakeholder discussions with participants during the events of the Fourth Singapore International Cyber week (SICW) as part of the regional consultations.

Multi-stakeholder exchange of views between GGE Chair and members, and non-governmental stakeholders during the SICW

Multi-stakeholder discussions on the topic "Strengthening International Cyber Cooperation" were held as part of the Leaders' Symposium during the SICW. The GGE Chair and Chair of the Open-ended Working Group were part of the leaders' panel together with Mr. Alexander Evans, Director Cyber, Foreign and Commonwealth Office of the UK, member of the GGE, and Mr. Emmanuel Rey Caintic, Assistant Secretary for Digital Philippines, Department of Information and Communications Technology, the Philippines.

During the Symposium, panelists provided their perspectives on the Group of Governmental Experts and Open-ended Working Group processes, how they should be complementary to each other and mutually supportive, and particularly focused attention on the issue of voluntary, non-binding norms in cyberspace, capacity building, transparency and confidence building measures.

It was noted that "cyberspace" was never designed to be secure – its creators were more concerned with ensuring fast, reliable connectivity, which is why cyberspace has now been exploited to the extent it has by malicious actors.

It was pointed out that given the current configuration of our global systems, cyber risks could be reduced but not entirely eliminated. If anything, malicious actors are as fast as or faster than defenders when it comes to using new technologies for attack. That means that better security in the cyber environment requires cooperation not only among States, but among all stakeholders. No country has all the tools to combat these threats alone.

However, it was also highlighted that cyberspace is not lawless and that measures developed within the UN and in other fora already provided a nascent framework for international cyber policy, including voluntary, non-binding norms of responsible State behavior, which need to be further developed.

Participants at the symposium further noted that States need to understand it is in their interest to observe cyber norms, since this would be a way in which the predictability of the behaviour of States could be established. However, it was also stressed that incentivizing the observance of norms that are voluntary in nature, including and in particular by non-state actors, would remain a challenge.

It was noted that the Association of Southeast Asian Nations (ASEAN) was moving ahead on implementing the voluntary non-binding norms of responsible State behaviour, and it was recalled that at the 2018 ASEAN Ministerial Meeting on Cyber Security, ASEAN countries had already agreed to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 GGE report.

Exchange of views between GGE Chair and members and ASEAN members and dialogue partners

The consultations between the Chair and members of the GGE took place within the context of the 4th ASEAN Ministerial Conference on Cybersecurity (AMCC). The AMCC was chaired by Minister Iswaran. Under-Secretary-General Fabrizio Hochschild Drummond, Special Adviser on the Preparations for the Commemoration of the Seventy-Fifth Anniversary of the United Nations, represented the United Nations, and the GGE Chair and Chair of the Open-ended Working Group were part of the high-level panel.

Participants highlighted that the threats emanating from cyberspace include State and non-state sponsored threats, cybercrime, and terrorist use of the internet. Hackers were easily available for hire to the highest bidder.

It was noted that in order to address these threats, there would be a need to go beyond traditional measures, although it was also stressed that preventive measures should always be balanced with issues such as respect for human rights and privacy.

UN processes, including the GGE and the OEWG, provided platforms for States to come together to discuss these issues. Participants noted the need to ensure complementarity between the GGE, which had a longer timeframe (ending in 2021), and the OEWG, which would complete its work in July 2020. It was highlighted that States had expressed the possible idea of also extending the OEWG.

It was noted that the GGE was perceived by some as an exclusive group. However, the mandate of the current GGE changes this perception by including consultations with States at the regional level and by holding informal consultations with all States at the UN headquarters.

In terms of efforts at the regional level, participants noted ASEAN's progress in building a rules-based cyberspace including through the implementation of the 11 voluntary, non-binding norms recommended in the 2015 GGE Report. Possible ways to implement the norms were discussed, together with the capacities that were required. It was noted that it would be important to take into account the different considerations of ASEAN Member States in implementing the norms.

Participants stressed that the interplay between norms and confidence-building measures could be considered further. An important next phase would be to translate norms and confidence building measures into practicable and implementable steps. It was suggested that States could make a stronger commitment to norms while allowing for the necessary flexibility in implementation.

It was also highlighted that the ASEAN Regional Forum (ARF) offers an important platform that could be used to enhance confidence-building measures. It was noted that the Forum had successfully developed a point-of-contact directory which would facilitate information exchange and cooperation between the ARF members as recommended in the GGE reports.[4]

Participants noted that a stronger framework was required, including to significantly scale up international initiatives and regional initiatives for international cooperation towards cyber security. In this endeavour, capacity-building would be key. It was underscored that capacity building is a two-way street where both the donor and beneficiary States would learn from each other.

It was noted that ASEAN had agreed to establish a working-level committee to consider the development of a long-term regional action plan to ensure effective and practical implementation of the norms including in the areas of CERT cooperation, protection of critical

[4] A/68/98, para 26 (c); A/70/174, para 16 (a).

information infrastructure and mutual assistance in cyber security. The committee was tasked to report back to the AMCC by next year on the specific areas of focus and the mechanisms to implement them.

The importance to continue building cyber capacity in ASEAN was highlighted. In this regard, support was expressed for capacity-building initiatives at the ASEAN-Singapore Cybersecurity Centre of Excellence in Singapore and the ASEAN-Japan Cybersecurity Capacity-Building Centre in Thailand. It was stressed that capacity-building efforts needed to go beyond governments to also include the private sector.

ASEAN dialogue partners made a commitment to continue to work with ASEAN countries to take forward to issue of cyber security in the region. It was noted that many excellent cooperative initiatives were already underway that could continue to be built upon. Participants also welcomed the partnership with the UN and other Dialogue Partners in this effort.

Summary of Discussions by the Chair of the GGE

At the end of the consultations, the GGE Chair summed up the discussions, noting that participants had:

- Indicated that cyber security is a growing concern of the international community and hence the UN GGE and OEWG processes provided an opportunity for States to discuss cyber security in a collective manner under the unique multilateral framework provided by the United Nations.
- Emphasized that traditional measures and negotiating formats for dealing with overarching global challenges amongst states may no longer be sufficient to deal with new threats emanating from cyberspace, due to the fluid and pervasive nature of the medium.
- Stressed the need for translating norms and confidence-building measures into practicable steps, that may evolve into better articulated, harmonized and robust systems or mechanisms for cooperative actions.
- Also stressed the importance of capacity-building measures for supporting implementation of accepted norms and principles involving all relevant and interested stakeholders and not only States, with a view to upholding peace, stability and security of cyberspace to the benefit of all.

The GGE Chair also highlighted that:

- Different regions have different priorities and perspectives on advancing the responsible behavior of states in cyberspace in the context if international peace and security.
- ASEAN is a region that has collectively taken important strides forward in implementing the 11 voluntary, non-binding norms of responsible State behaviour as contained in the 2015 GGE report. It would be key to engage States of the ASEAN region on their priorities and interests on the issue of ICTs in the context of the ongoing UN processes.
- In this regard, he looked forward to focused and streamlined contributions from ASEAN on ideas and lessons learned and, if possible, to a briefing on the work of the ASEAN working-level committee on norms implementation.