The objective of the Informal Multi-stakeholder Virtual Dialogue Series was to support the ongoing discussions at the UN Open-Ended Working Group (OEWG) on developments in the field of information and communication technology (ICT) in the context of international security.

Informal Multi-stakeholder Cyber Dialogue

Summary report

04-10 December 2020

Taking place in a new virtual format, the Informal Multi-Stakeholder Cyber Dialogue was an initiative of the multi-stakeholder community and a number of UN member states. The dialogue series (04-10 December) was intended to complement the OEWG, but it is not a formal part of the OEWG process.

As a platform for dialogue between non-government organizations (NGOs), technical experts, civil society, the private sector and states, this series of thematic sessions aimed to:

- Collect non-governmental stakeholder perspectives on the UN Open-Ended Working Group (OEWG) pre-draft, and
- Create opportunities for in-depth dialogue between State and NGO communities on the themes of the OEWG.

Participation in the event was open to all interested stakeholders.

This document collates the summary reports of each of the session events, as well as the report of a side event. Further information about the series, including the video recordings, are available on the dedicated event website: www.letstalkcyber.org

INTERNATIONAL LAW

04 December
SESSION REPORT

GENERAL SUMMARY

13:00 UTC
Co-chairs

- Japan
- Oxford University

There were a total of 286 participants who joined the event from Zoom and the Livecast including government representatives, non-governmental organisations, academia, and private sector stakeholders. The Livecast attracted viewers from 28 countries and 41 cities around the world.

SESSION OUTLINE

Takeshi Akahori (co-chair, Ministry of Foreign Affairs of Japan) kicked off the session with an explanation of the content of the 2013 and 2015 GGE consensus reports and of the pre-draft report under consideration by the OEWG on applicability of international law in cyberspace. He particularly highlighted language in the pre-draft concerning state responsibility, self-defense and international humanitarian law.

Dapo Akande (co-chair, Oxford University) set the scene of the session by explaining (i) how as a general matter international law applies to the activities of States and non-state actors in cyberspace; and (ii) attempts to clarify - outside the UN processes - the applicable international law rules. On (i) he mentioned why it is that international law applies by default to state activity whether in cyberspace or elsewhere as well as how international law applies to activities of non-state actors, focusing on rules of attribution and the due diligence obligation of States to prevent harmful cyber activities by non-state actors. On (ii) he mentioned the Tallinn Manual and the recent work that Oxford and others have been engaging in to clarify the rules with regard to particular types of harmful cyber operations.

Marietje Schaake (Cyber Peace Institute) indicated that while cyberattacks often stay below the thresholds of intervention or armed conflict, creating ambiguity, there is a wide range of laws and rights that might be at stake below those thresholds, including human rights, non-proliferation, counterterrorism, crime fighting, etc. Introducing the work of the Cyber Peace Institute, she stressed that enough information in the public domain was necessary for accountability to become the goal. She thought that in addition to the United Nations, groups of like-minded nations could work together for example on the rule of law principles and look at how they could crack some politically sensitive issues. She also recognized the need to build capacity and institutions for attribution.

Liis Vihuul (Cyber Law International) pointed out that the international community has had an expectation that countries would start articulating what kind of practical implementation of the

international law, rights and obligations can and should be expected of States in the cyber context but that progress was modest. She believed that international peace and security would be better served if countries would be more willing to accept that international law provides substantial prior restrictions that take off the table, certain types of cyber operations. With regard to States that feel that the international legal debate lacks inclusivity, in part because those countries do not have the capacity to fully and meaningfully participate in the international negotiations concerning international law, she said that to a great extent, "the ball was in their court" because in many countries there was room for improvement with regard to internal coordination.

Harriet Moynihan (Chatham House) suggested that to make progress in discussions on how international law applies, more States needed to put on record their views on how particular principles of international law apply, where possible with reference to concrete examples. She gave a few examples of areas on which it would be good to have States' views. Those areas were non-intervention (could interference in elections, cyberattack on medical facilities constitute intervention and was the victim state entitled to take countermeasures?), peaceful settlement of disputes (do the Security Council and the ICJ provide a basis?).

Tilman Rodenhäuser (ICRC) recalled that international humanitarian law (IHL) applies to cyber operations during armed conflict. On the pre-draft under consideration in the Open-Ended Working Group he said that ICRC attaches great importance to some of the statements or the findings, including that "IHL reduces risk and potential harm to both civilians and combatants in the context of armed conflict", and that "IHL neither encourages the militarization nor legitimizes resort to conflict in any domain." (paragraph 29), and that there is a need to fully clarify questions relevant to how the principles of IHL, such as principles of humanity, necessity, proportionality, distinction and precaution apply to ICT operations in the context of an armed conflict (paragraph 32). ICRC believed that finding agreement among States on how international law, including IHL, restrict cyber operations during armed conflict is of utmost importance. He encouraged States to deepen their discussions on how IHL applies in cyberspace and indicated that the ICRC and other multi-stakeholder entities were available to contribute to these discussions as needed.

Jan Neutze (Microsoft) recalled that the first United Nations organized multi-stakeholder meeting on trust and security in cyberspace held a year ago in New York in the context of the Open-Ended Working Group which included a formal role for non-state organizations to contribute to the discussions was a remarkable milestone. He explained that since then there were a number of additional positive steps such as the UN Secretary General's Roadmap on Digital Cooperation, the increase in organizations endorsing the Paris Call for trust and security in cyberspace which was originally adopted in 2018, and the Oxford University research project and its three statements. He emphasised that governments need to be the ones that that agree on norms and apply them with data and other input from companies and that the world in many ways is running out of time before offensive cyber capabilities are applied against a critical infrastructure target and will cause significant impact and consequences. He urged all digital citizens to get involved.

The above statements were followed by active interaction with other participants. Issues raised included the importance of publishing national position papers, how to maintain a peaceful cyberspace, cyberattacks on medical facilities and IP theft on medical research projects,

whether disinformation constitutes intervention, criminal responsibility of non-state actors under international law, the right of taking collective countermeasures.

MAJOR THEMES / AREAS OF CONVERGENCE

As affirmed in the 2013 and 2015 GGE reports, international law applies in cyberspace. The ongoing OEWG and GGE are expected to further clarify how international law applies in cyberspace. At the same time, considering that there is a realistic limit to what can be agreed by States in the OEWG and GGE, efforts by like-minded countries or discussions involving the multi-stakeholder community are also important. Academia also plays an important role in such discussions and can provide in-depth studies and research.

States are urged to publish their position papers on how international law applies in cyberspace. Differences in national positions on how international law applies in cyberspace will not harm the common understanding that international law applies in cyberspace.

Civil society has an important role to play in discussions concerning how international law applies, including by providing data and examples.

AREAS FOR CONTINUING DISCUSSION:

Is there a need to establish an international attribution mechanism? Could existing mechanisms including the Security Council and the International Court of Justice be used in disputes involving cyber activities?

RECOMMENDATIONS

The OEWG report should devote some lines to the impact of the COVID-19 pandemic on discussions related to application of international law in cyberspace.

RULES NORMS AND PRINCIPLES

07 December

SESSION REPORT

GENERAL SUMMARY

15:00 UTC
Co-chairs

- Canada
- Global Partners Digital (GDP)
- Microsoft
- Association for Progressive Communications (APC)

There were a total of 319 participants who joined the event from Zoom and the Livecast including government representatives, non-governmental organisations, academia, and private sector stakeholders. The Livecast attracted viewers from 22 countries and 32 cities around the world.

SESSION OUTLINE

The session opened with a scene setter by Sirine Hijal and Daniel McBryde of Global Affairs Canada (GAC). Sirine Hijal presented the 11 norms of State behaviour in cyberspace agreed by the UN Group of Governmental Experts (GGE) in its 2015 report. Dan McBryde then outlined the 2016-17 GGE draft text on norms and Canada's proposed norms guidance text at the current OEWG.

The scene setting remarks were followed by statements by Sheetal Kumar, Global Partners Digital (GDP) and Veronica Ferrari, Association for Progressive Communications (APC) made on behalf of stakeholders who submitted input to the OEWG on the norms non-paper proposals. GPD and APC's statement emphasized three key comments on the norms text from the joint stakeholder input: a) humans are the ones impacted by state behaviour in cyberspace and therefore a human-centric and rights-based approach to norm implementation is needed 2) cyberspace isn't equal: cyber incidents impact people in a differentiated manner, c) Relevant discussions, including regarding implementation, need to be open, inclusive and transparent.

Nemanja Malisevic shared the industry perspective on the issues at stake. Microsoft's statement reiterated the importance of multistakeholder initiatives and called for a more systematic involvement of all relevant stakeholders. It further invited states to reaffirm the validity of the 11 norms recognized by the 2015 UNGGE in their entirety. It also encouraged states to explain what the implementation of these norms is expected to look like, and stressed that states should strive to turn these politically binding commitments into legally binding rules.

The statements were intended to provide context for the open discussion which followed and which was based on the following four questions:

1. In the non-paper, there is guidance for the implementation of the eleven agreed norms. Are there any elements missing in this guidance?
2. The focus so far in the non-paper is on the 11 agreed norms, but are there other issues that should be considered?
3. What challenges do you see in taking forward the proposals included in the non-paper, including in any of the relevant norms guidance text?

4. With respect to the draft “Norms" section of the OEWG the pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree? (see paragraphs 38-44) In particular, do you think there is sufficient reference to non-governmental stakeholder engagement? If not, how could this be improved?

MAJOR THEMES / AREAS OF CONVERGENCE

- *The implementation of what has already been agreed is of primary importance*: It was widely agreed that there should be no ‘unravelling’ the existing agreed 11 norms. Norms guidance, like that provided by Canada and other states, as well as other stakeholders, is important at this stage for operationalisation of the norms.
- *Inclusivity of stakeholders in the implementation of norms:* the operationalisation of norms should not be ‘top-down’. Stakeholders, including the technical community and civil society, should be involved. For example, they possess information necessary to ensure the stability and security of the internet. Input from all relevant stakeholders should be systematic, rather than ad-hoc.
- *International law and norms are complementary:* Voluntary norms do not affect the obligations states already have under international law; instead the norms and international law are complementary. Implementation of the norms can support state’s compliance with their international legal commitments.
- *Accountability is needed:* When agreed cybernorms are not respected or violated, there currently isn’t sufficient accountability for those who violate the norms. This is important for the implementation of cyber norms; otherwise, the norms fail to have real-world impact without frameworks that ensure they are implemented and not violated. Engaging participants from the multistakeholder in implementation efforts can support those efforts.
- *A human-centric and bottom-up approach should support the implementation of the agreed norms:* as it is humans who are impacted by state behaviour and cyber incidents, it is important for states to ensure that human rights are a core part of norm implementation. The implementation of norms should also take into consideration that cyber incidents impact people in a differentiated way because of existing inequalities. Women, as well as people of diverse sexualities and gender expression, are more often targets of online violence. Increasingly, disinformation campaigns further alienate minority groups.
- *Regional organisations play an important role in norms implementation:* Regional organisations can play a range of roles in supporting norm implementation, including through developing frameworks for implementation that are tailored to regional context and gathering of best practices. They can complement what is being done at the UN/global level. However, in supporting member states to implement cyber norms, they should engage all stakeholders.

AREAS FOR CONTINUING DISCUSSION:

- **Norm elaboration:** There was discussion regarding whether the guidance related to norms on critical infrastructure could be further elaborated, specifically to include reference to electoral and health infrastructure. There were different views expressed: some felt that referring to electoral and health infrastructure would be singling these sectors out, and would therefore give the impression that other sectors should not be understood to be protected in the same way. However, others felt that the inclusion of language such as “including, but not limited to” would be sufficient to ensure that any interpretation of the norms on critical infrastructure would not be limited to specific sectors only. In addition, a question was raised regarding the “public core” norm which has been proposed by the GCSC, how it is perceived and whether it is seen as key to norm implementation.
- **Norm implementation vs a binding agreement**: There was some discussion as to whether the implementation of the norms is sufficient to guide State behaviour in this space, or whether the current framework needs to be supplemented by the elaboration of either a legally binding

instrument or additional norms. While there was no agreement on this, a point was made that continuing implementation of the norms could reveal any potential gaps and thereby potentially help identify new norms that may be needed. Some States and participants in the event indicated that they believe that the current framework of law and norms is not sufficient and that a treaty or binding instrument is needed to regulate State behavior in this space, but they recognized that such a treaty is unlikely to be adopted anytime soon, given that a majority of States continue to oppose such an approach.

- **International law thresholds and impact on norm implementation**: A question was raised regarding what thresholds need to be reached for specific elements of international law to apply and how the understanding of what these thresholds are impacts norm implementation. While not discussed in-depth, this could merit further discussion as it could help clarify the interplay between existing agreed norms and international law.

RECOMMENDATIONS FROM STAKEHOLDERS

- States should prioritise the implementation of the existing agreed 11 norms, utilising guidance developed within the OEWG and engage other stakeholders in doing so. However, in doing so, they should not discard the necessity of exploring whether additional norms may be needed at some point or how such norms may be turned into legally binding commitments in the future.
- Mechanisms set up to support implementation of the norms should institutionalise stakeholder engagement, including involvement of the technical community, civil society and industry.
- The OEWG report should include reference to the role of non-governmental stakeholders, including civil society, academia, the technical community and industry, in supporting the implementation of norms, rules and principles.
- The OEWG's report recognises the differential impact of cyber incidents on marginalised groups, but it should further elaborate on these concerns.
- States should consider the links between human rights and cyber norms and comply with their obligations under international human rights law when operationalising cyber norms.

EXISTING AND EMERGING THREATS

08 December
SESSION REPORT

GENERAL SUMMARY

01:00 UTC
Co-chairs

- Australia
- Indonesia

The United Nations' Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security is mandated, among other things, to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them.

This session, co-chaired by Indonesia and Australia, aimed to provide an opportunity for the multi-stakeholder community, including civil society, academia, industry and the private sector, to brief UN Member States on existing and emerging cyber threats, with a focus on those most likely to impact international peace and security.

The session attracted a broad participation of 180 people who joined from Zoom and the Livecast representing governments, civil society, academia, and the private sector. The Livecast attracted viewers from 17 countries and 25 cities around the world.

SESSION OUTLINE

The session opened with introductory remarks from Rolliansyah Soemirat, Director for International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia and Johanna Weaver, Special Advisor to Australia's Ambassador of Cyber Affairs and Critical Technology, and Head of Delegation to the OEWG and Group of Government Experts, Department of Foreign Affairs and Trade Australia.

The session included civil society, academia and industry presentations from: Jeremy Thompson, Executive Vice President & Deputy Cyber Security Officer Huawei Western Europe; Yihao Lim – Principal Intelligence Enablement Consultant (Asia Pacific) FireEye; Anastasiya Kasakova – Public Affairs Manager Kaspersky; Jessica Woodall – Cyber & National Security Senior Analyst Telstra; Benjamin Ang – Senior Fellow, Cyber and Homeland Defence Programme of CENS Centre of Excellence for National Security, RSIS Singapore; Gunjan Chawla – Programme Manager Centre for Communication Governance National Law University Delhi; John Hering – Senior Government Affairs Manager Microsoft and representative of the Cybersecurity Tech Accord; Maarten Van Horenbeeck – Board Member and former Chairman of the Forum of Incident Response and Security Teams (FIRST), Arindrajit Basu – Research Manager Centre for Internet&Society India, Georgia Turnham and

Eric Pinkerton – Trustwave; Stéphane Duguin – CEO CyberPeace Institute; and Paul Meyer – Senior Advisor, ICT4Peace.

A set of guiding questions was distributed in advance in order to inform the contributions of participants. Presenters were asked to address the following questions:

1. What cyber/ICT related activities do you assess to be the biggest threat to international peace and security?
2. With respect to the draft "Existing and Emerging Threats" section of the OEWG pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree?

Presentations were followed by small panel discussions moderated by discussants from: Arina Pazushko – Head of Brand Development BI.ZONE, Farlina Said – Analyst Foreign Policy and Security Studies ISIS Malaysia, Dr Fitriani, CSIS Indonesia.

Presentations and panels were followed by an interactive question and answer session from participants and panellists. All views expressed during the session represented the views of the individuals or organisations who expressed them, and not those of the chairs, sponsors or partners.

MAJOR THEMES / AREAS OF CONVERGENCE

Presentations were wide-ranging in their assessment of the cyber threat landscape. Themes that cut across several presentations and panel discussions of existing and emerging threats included: the centrality of trust; importance of transparency; risk of escalation and risk of balkanisation; the disproportionality of cyber risk; and the delineation of threats within or outside the mandate of international peace and security.

Presenters and panellists provided the following key points to summarise the session:

- Trust is a key asset in tackling emerging threats in cyberspace
- The ability to respond to threats posed by ICT and cyber developments are restricted by the same difficulties as conventional efforts to maintain peace and stability, and reliant on nation states being transparent about their capabilities, in a time when we are seeing a declining trend in transparency around State cyber policies
- The digitalization of smart devices can escalate the physical threat of malicious cyber activity
- Continued incidents of malicious cyber activity despite deterrence and response efforts
- The escalation of threats from dual-use goods, surveillance technologies, and democratisation of military cyber capabilities could undermine human rights
- The difficulties associated with differentiating between state and non-state actors
- International peace and stability can also be impacted by other related issues:
    - There is a growing concern and need to address the issues of misinformation and access so all people can enjoy the benefits of ICT safely
    - Deep-fake technology can exacerbate the impact of information operations
    - The need to differentiate and distinguish between the development and deployment of offensive cyber capabilities on the one hand, and the varying

roles of corporations as non-State actors in the ecosystem as vendors of ICT equipment and services on the other hand.

RECOMMENDATIONS

Presenters, panellists and participants provided the following recommendations in the course of written or spoken comments and questions during the session. These points do not constitute formal recommendations of the session's chairs, sponsors or partners:

- The building and maintenance of trust in cyberspace should not only focus on states but also on non-state actors, private sector, communities and individual users
- Governments and law-makers should be encouraged to set minimum requirements for cyber security, and create labs and test centres to encourage innovation
- The multi-stakeholder community, including states, should work on global standards for cyber security rather than bifurcate into regional standards
- Measures to promote responsible state behaviour in cyberspace should be accompanied by greater accountability
- The UN should move from general discussion of cyber threats to measures that mitigate or eliminate those threats. In this regard, the "Programme of Action" represents a concrete way forward
- All stakeholders should address the escalation of threats to human rights being undermined in cyberspace
- Further and continuing dialogue including all multi-stakeholders is needed to shed light on current and future threats and promote a collective approach to developing solutions.

CYBER POLICY CAPACITY BUILDING

8 December 2020

SESSION REPORT

GENERAL SUMMARY

12:00 UTC
Co-chairs

- Department of International Relations and Cooperation of the Republic of South Africa
- EU Institute for Security Studies
- Research ICT Africa

The discussions in the OEWG to date have reaffirmed the role of cyber capacity-building (CCB) in addressing the systemic, transnational risks and vulnerabilities associated with the digital transition, the lack of ICT security, disconnected technical and policy capacities at the national level, as well as the associated challenge of digital inequalities. States have also noted that in addition to technical skills, there is a pressing need for building expertise across a range of diplomatic, policy, legislative and regulatory areas.

The main objective of the session was to dissect problems, needs, and ways forward to achieve meaningful participation of all countries involved in discussions on disarmament, peace, and stability in cyberspace. Building on the agreement that "*International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use*"[1], the session unpacked problems, needs, and way forward of this engagement[2]. Some of the issues at stake include prioritisation based on needs assessments, the focus on policy in CCB, the identification of mechanisms for the sustainability of funding and skills transfer, the development of impact metrics, and the nexus between development and security.

In order to ensure balanced perspectives, the session included speakers from Morocco, South Africa, Nigeria, the EU, India, Brazil, the UK, and Australia. The Co-Chairs also shared a resource pack of cyber capacity building initiatives on policy across the world prepared in cooperation with the Global Forum on Cyber Expertise (GFCE) and invited Member States and other stakeholders to add to these initiatives and to increase commitments to what exist. The resource pack is available at the conference website: www.letstalkcyber.org. The session attracted a broad participation of 271 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 23 countries and 33 cities around the world.

SESSION OUTLINE

[1] UNGA (2015:10). A/70/174
[2] See objectives and guiding questions of the session in the concept note available at https://eu-iss.s3.eu-central-1.amazonaws.com/horizon/assets/BpIVojEd/concept-paper-ccb-final.pdf

Many of the ongoing efforts undertaken globally focus on strengthening and delivering technical, institutional and legislative capacities. However, while international partnerships and cooperation are often recognised as a key element in the national or regional cybersecurity strategies or policy frameworks, this aspect has been so far neglected in the international approaches to cyber capacity building. The limited capacity of certain parts of government to fully participate in international cyber policy discussions creates an obstacle for governments to fully embrace whole-of-government and whole-of-society approaches, on the one hand, and limits their capacity to represent their country's positions, on the other hand. The session reiterated the importance of representation, local ownership, and evidence-based strategic objectives and goals.

Part I: Designing an inclusive CCB agenda: issues, interests and priorities

1. The session enquired on whether thinking about CCB in terms of the best practice paradigm was optimal as these cyber security best practices might not be applicable to a variety of national contexts. Nevertheless, the session highlighted certain principles such as the diversity of stakeholders and the important role of the private sector, the need for research to measure impact, and the inclusion of the sustainable development goals.
2. The 2030 sustainable development goals (SDGs) were emphasised considerably, in particular goal 4 on inclusive and equitable education and the promotion of lifelong learning for all and goal 5 on achieving gender equality and empowerment for all women and girls receiving the top spot. Several speakers agreed on the need to encourage Member States to mainstream the SDGs in all UN discussions. The session recognised also that the inclusion of language on SDGs within the First Committee mandating resolutions was an indication that the whole of UN approach embracing all the pillars of human rights, security and development should be applied also to CCB.
3. The session acknowledged the disproportionate attention given to technical issues related to cybersecurity. The participants agreed that there is a need to bridge technical CCB and policy by also educating the technical community on the policy issues and vice-versa. To this end both technical and policy communities must establish ways of engaging and setting CCB priorities.

Part II: Moving towards a more balanced CCB agenda: state of play and possible pathways

4. The session focused on the donor, implementer and beneficiary relationship. It highlighted the importance of local ownership of capacity building even extending to medium of instruction. Language was recognised as an important aspect and this issue was highlighted by the fact that as countries develop National Cybersecurity Strategies, these only serve the purpose of building trust and transparency when they are understood globally which means the use of common concepts and the need for translation into certain languages, often English. There should also be more efforts by implementers and donors to develop and implement CCB activities in other languages and create resources in those languages too to help with the establishment of a common baseline and understanding of key principles.
5. For countries that do cyber capacity building independently, domestically and regionally, partnerships should be able to meet them where they need and sometimes it is in translation services. A comprehensive set of CCB initiatives and services on offer should reflect this

principle.

6. Priorities of Member States for cyber capacity building differ and the session highlighted that these have more to do with the local realities than global narratives and likewise, CCB stakeholders respond more to the local needs rather than to global principles. At the core of all, capacity building relationships are based on trust and partners should not seek to expedite programmes at the expense of building trust which can be harnessed and nurtured over a long period of time.
7. The session highlighted the need to increase transparency at the implementation level by drawing from local expertise so that on the one hand, cyber capacity building goes beyond one-off workshops and interventions; on the other, financial resources circulate in the beneficiary countries as well. This triangular level of relationship of donor, implementer, beneficiary contributes to building trust, accountability and sustainability. The session highlighted how sustainable, strategic and long-term funding can be instrumental to these efforts. One that is also flexible where needed and open to an appropriate mix of mechanisms, including modalities and selection procedures.
8. The important concept of responsible solidarity as the idea of mutually agreed partnership goals and capacity building priorities emerged. The session also highlighted the need for this solidarity or partnership to be approached as a process and not an event and in this regard, the relationship should begin even at the scoping phase to identify gaps and solutions.
9. The issue of differing priorities between donor and beneficiary was discussed, and peculiarities in different regions. Speakers suggested that a baseline of principles should be part of the relationship and these include the respect for human rights, freedom and participation of civil society amongst others. The key reference in terms of a partners' commitment to these priorities are accessions to various UN and regional Conventions and Protocols.
10. In the spirit of politically neutral capacity building, participants raised the issue of the need for a more contextualized approach to capacity building when linked to specific legal instruments or conventions, especially when certain conditionality is attached. While these are some of the ways to achieve harmonisation across a policy area, it is important to better explore the trade-offs that such approaches to policy capacity building create.

Part III: The world of 100% capacity: is the international community ready?

11. The primary question raised during the session was whether the future CCB efforts should focus on strengthening capacities for the implementation of the provisions in the OEWG and UNGGE reports or whether it should rather focus on strengthening the capacity of the recipient countries to be more independent actors in the future discussions. Speakers noted that the OEWG draft pre-report does not give a clear answer in this regard and includes a double objective: a) to support states in adhering to their international commitments and creating resilient, secure and peaceful ICT environment; and b) in order to support states in developing their own understandings of international law, norms, etc.
12. Regarding the need for capacity building partnerships that reflect nationally identified needs and priorities, the discussion revealed that while some efforts might be perceived as insufficiently reflecting the local needs, many countries consider the conversation to be driven by different groups. Participants reinforced that the direction and substance of CCB is being shaped by all Member States. For instance, it was highlighted that some countries from the global South actively participated in the past three GGEs and provided substantive input with the global South in mind.
13. The session agreed that achieving full cyber capacities is an ambitious goal that is hardly

possible to achieve given the speed of technological innovation and evolution of the threat landscape. This challenge is equally valid for all countries independently on the stage of their development.

14. It was clearly recognized that the OEWG provided a platform for Member States that had previously been absent from the global discussions about cyberstability and responsible behaviour in cyberspace. The key take-away was that more voices will strengthen the accountability and transparency of the whole system.
15. Several speakers have stressed the role that regional organisations play in delivering cyber policy capacity, in particular through convening the right actors, ensuring more contextualized support and strengthening the local ownership dimension. However, their role is often hindered by the fact that the mandates reflect all Member States' maturity. Member States determine how fast or slow regional organisations should take up the role of CCB. The session also highlighted that while the global UN discussions may move at a certain pace, regional organisations interface closer with Member States and are able to move at the pace wherein no Member State is left behind.
16. While we 'wait for 100% capacity', there is a need to reflect on CCB priorities and how they evolve, in particular to ensure that the initial objectives and developmental goals are not undermined by more short-term policy considerations. In this, the research community will play an important role as part of the multi-stakeholder community in the OEWG and in CCB discussions.

MAJOR THEMES/AREAS OF CONVERGENCE

a) CCB and ICT related capacity building priorities have evolved since the early 2000s. It is important to understand how and why these changes occurred and what is their impact on the global cyber capacity efforts.
b) CCB are not once-off initiatives but rather a continuous and sustained endeavor and an integral part of National Cyber Strategies and of their reviews.
c) The 2030 sustainable development goals are key areas for cyber capacity building in the context of international security. A special focus must be paid to SDGs 4 and 5.
d) Member States should shift attention to capacity building on policy issues by bridging gaps between technical and policy communities
e) The relationship between donor, implementer and beneficiary to deliver cyber capacity building should be based on trust and transparency.
f) Local ownership of cyber capacity building is important for sustainability. This includes skills transfer for local implementation of CCB programmes and funding management.
g) Cyber capacity building programmes like development and sharing of National Cyber Security Strategies only serve the purpose of building trust when they are widely understood in a common language. Translation of Strategies into UN official languages and their publication in UN Platforms is a substantive and administrative priority.
h) Despite divergences and peculiarities on CCB priorities, the respect for human rights and participation of civil society must form the basis of partnerships.

REGULAR INSTITUTIONAL DIALOGUE

09 December 2020
SESSION REPORT

GENERAL SUMMARY
15:00,UTC
Co-chairs

- France
- Egypt
- Women's International League for Peace and Freedom (WILPF)
- Kaspersky

The United Nations' Open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security has provided UN Member States with an open and inclusive forum to discuss international cybersecurity. Identifying a regular mechanism to continue dialogue on this subject is an urgent priority and may represent one of the OEWG's most significant outcomes.

This session, co-organised by France, Egypt, Women's International League for Peace and Freedom (WILPF), and Kaspersky, invited discussion and inputs from non-governmental stakeholders on the topic of regular institutional dialogue (RID). The main purpose was to discuss different possible types of frameworks and institutional settings in which the global community can continue to address threats associated with the use of information and communications technologies (ICTs) in the context of international security and peace, including with a possible of meaningful engagement and participation by relevant non-governmental stakeholders.

The session attracted a broad participation of 150 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 17 countries and 32 cities around the world.

SESSION OUTLINE

Brief opening remarks were provided by representatives of the four co-organisers: Bassem Hassan, Counsellor, Permanent Mission of Egypt to the United Nations; Allison Pytlak, Programme Manager, WILPF; Henri Verdier, Ambassador, Digital Affairs, Ministry for Europe and Foreign Affairs, Government of France; and Anastasiya Kazakova, Public Affairs Manager, Kaspersky.

The session was moderated by Camille Morfouace-de Broucker, Ministry for Europe and Foreign Affairs, France.

A set of guiding questions was distributed in advance in order to inform the contributions of participants. The questions were organised under two themes: Ideas for a regular Institutional Dialogue; and Stakeholder participation—lessons learned and challenges.

Following the opening remarks, participants were invited to respond to a Mentimeter poll that asked, "What topics should future regular institutional dialogue aim to cover?" Participants could select multiple responses from the answers provided.

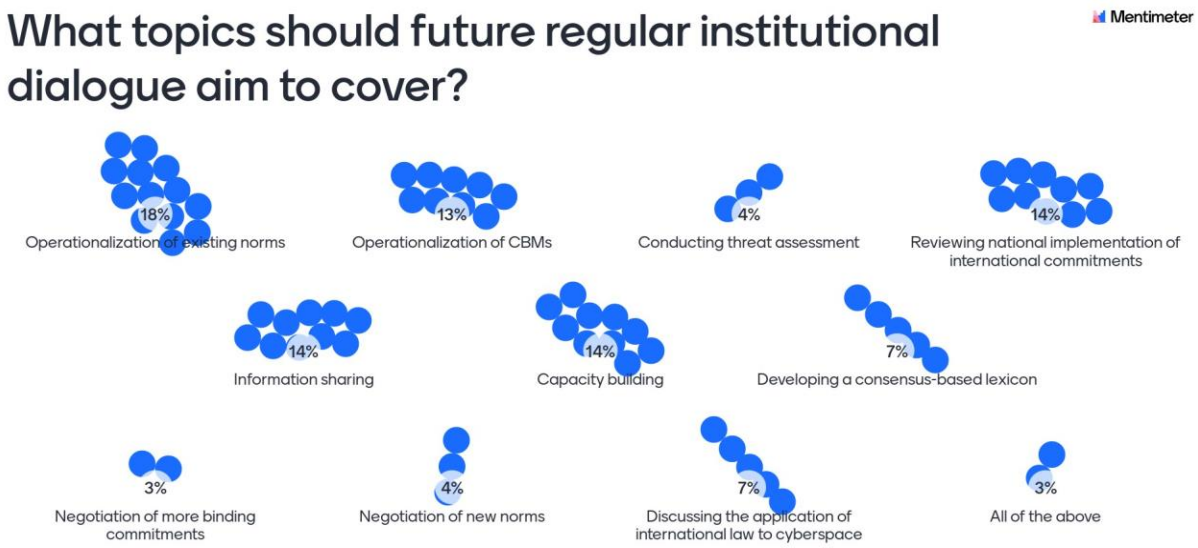
The moderator then opened the floor for discussion and questions. Some participants asked questions of the speakers while others took the floor to express views and/or positions on key themes. These questions and points were either conveyed through the chat function, including by individuals watching the livestream, or asked directly on video. Toward the end of the session, Ms. Kazakova shared the results of the poll. They are presented in the next section of this summary.

MAJOR THEMES / AREAS OF CONVERGENCE

As noted by the panellists of Egypt and France, there is growing convergence among UN Member States around five key characteristics that future RID should account for: (i) be inclusive, i.e. allowing all countries to participate and contribute; (ii) be regular with a timetable for the meetings; (iii) be institutional with clear points of reference and rules of procedures; (iv) be consensus-driven to ensure universality of a platform and adherence to its outcomes; and (v) be action-oriented in order to move further to practical outcomes after several years of discussion of key theoretical and fundamental principles.

All participants who spoke during the session, as well as the panellists, seem to agree on two important topics for future RID to focus on: ***national implementation of previously agreed non-binding norms*** (including the monitoring and reviewing the national implementation efforts) and ***capacity-building*** (for ensuring that the UN Member States have enough capacity for norm implementation). The panellists all emphasised the importance of transparency and inclusivity. There was also wide acknowledgement that ***multi-stakeholder participation*** plays a crucial role in the operationalisation of norms and confidence-building measures (CBMs) as states cannot alone achieve international security and peace in relation to the use of ICTs. However, it was noted that the current set-up of the OEWG does not always allow for non-governmental actors to meaningfully participate and support the discussions between UN Member States. Therefore, it is important for the future dialogue to move from discussions on 'if' the multi-stakeholder engagement is possible to 'how' this can be organised.

The poll results reflect the views of the speakers:



However, roles are different within the international community, both between governments and non-governmental stakeholders, but also among different stakeholder groups. Particularly, the private sector and industry, as noted by Kaspersky, seems essential in the operationalisation of norms related to critical infrastructure protection, ensuring the integrity of supply chains, responsible reporting of vulnerabilities, and discussing cooperative mechanisms for a global response in the event of a significant cyber incident or attack. The role of the civil society, as stressed by WILPF and many participants, is to bring forward the voices of those that are affected by the issue as well as bring those stakeholders who have the necessary expertise for the discussions. WILPF shared examples of how non-governmental stakeholders engage and participate in other multilateral and UN fora on international security issues.

Finally, as expressed by all panellists, it is time to achieve more practical outcomes. In this regard, a proposal that is now cosponsored by 47 UN Member States and supported by many other Member States to establish a Programme of Action[3] (PoA) has been initiated by the delegations of France and Egypt. This proposal was discussed as an instrumental way for RID that can move UN discussions on international cybersecurity forward. To a question from one non-governmental participant on how the PoA can be implemented practically, the panellists from Egypt and France explained that there is currently a lack of knowledge about national implementation of the UN cyber norms which makes such a PoA a unique opportunity to monitor implementation and identify the gaps in implementation, the normative base, and capacity. As one possible option for a standardised reporting template, national implementation could be also conducted through the national survey, such as proposed by Mexico and Australia during OEWG discussions.[4] In the chat, one governmental participant shared that it and another Member State have submitted to the OEWG an overview of how each country implements the norms. France also noted that for the future RID, although implementing the cyber norms is crucial, reaching a global treaty is not a priority as the discussion of the treaty only hinders the actual implementation of norms and having one treaty only would hardly allow to face the multitude issues in cyberspace.

---

[3] *The future of discussions on ICTs and cyberspace at the UN*, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

[4] *Joint Proposal*, 16 April 2020, https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf.

Some questions and remarks from participants raised issues that may require further consideration, elaboration, or work. Some examples include: how to gain support for a PoA from countries like Russia, China, and the United States; how the timeline to potentially negotiate and adopt a PoA will align with the forthcoming (second) OEWG, as well forums like the Internet Governance Forum (IGF) and the Paris Call; what a PoA can do to guard against the militarisation of cyber space and avoid becoming an instrument that regulates cyberwarfare; accounting for the lack of an attribution framework; if the UN is the best place to coordinate cyber capacity-building; and what specific modalities are needed to ensure *meaningful* participation of non-governmental stakeholders.

RECOMMENDATIONS

The following points reflect substantive suggestions and recommendations made by panellists or the participants in the course of written or spoken comments and questions. They do not constitute formal recommendations, unless presented as such.

From organisers/panellists:

- Be inclusive of all UN member states and allow for meaningful participation by non-governmental stakeholders. Openness and transparency are important considerations. This was emphasised variously by all panellists.
- It's time for action-oriented dialogue and/or processes, and a move away from deliberative processes like Groups of Governmental Experts and the OEWGs on theoretical and fundamental questions. These types of fora are not designed to take the kind of action that is needed on this issue at this juncture, such as reviewing or monitoring national implementation of the UN cyber norms, as one example. Additional thematic tracks of work could potentially be based on those that have been established within other initiatives such as the Paris Call.
- A global framework is needed, to pull together and give impetus to what exists regionally, or otherwise.
- Learn from good practices in non-governmental engagement in other international security fora. This includes modalities that enable stakeholders to engage in real-time, rather than in a single allocated session; enable space for side events or expert panels; and agree on standing rules for participation, as part of rules of procedure.
- Continue working on the consensus-based guidance for the implementation of the previously agreed norms (including norms on critical infrastructure protection, supply chain integrity, and responsible reporting of vulnerabilities); resolve questions about what a "cyber conflict" is, among other key concepts; and develop a consensus-based lexicon including on dispute-settlement, despite the challenges of doing so.
- Learn from other PoAs and their implementation. For example, they can eventually lead to legal instruments if needed; they can bring a diverse patchwork of existing regulations under one umbrella; and national implementation needs to be the priority.

From participants:

- The forum created by the PoA could serve for consultation and provide a dispute settlement mechanism, but to do so in a timely way it would have to be able to convene as required and not just in an annual meeting. The PoA could also evolve into a UN Cyber Security Committee, supported by a UN Office of Cyber Affairs.
- It was noted that the Human Rights Council's Universal Periodic Review (UPR) process, which is comprised of state reports and independent review, provides an

interesting model for promoting and supporting implementation of agreed norms, even those that are "voluntary and non-binding" such as those contained in the 2015 GGE report. The PoA could consider developing a similar mechanism as a result, or part, of the PoA, such as one non-governmental participant has already proposed.

- It was asked if the PoA could establish a mechanism for emergency and current risks, such as the current threats to a vaccine supply chain, for example. The same participant noted that this would not need be like the UN Security Council, but more operational.
- A participant wrote that a programme of work is needed, rather than a programme of action. This participant encouraged reaching a balanced normative framework and common understanding on how international law applies; after which a legally binding framework is needed "to achieve real accountability and legal deterrence."
- One participant suggested that the PoA should also report progress to the IGF throughout the year.
- It was suggested to establish a "committee of peaceful digital space in United Nations to develop [an] international treaty on Data, Governance, Security, Crime" which could be modelled on the International Civil Aviation Organization or inspired by the UN Convention on the Law of the Sea or the Committee on the Peaceful Uses of Outer Space (COPUOS).
- While this dialogue series is important, it shouldn't become the norm for non-governmental stakeholders and supportive governments to organise dialogue opportunities outside of what is happening at the UN in order to be involved in the discussions. Such dialogue should be institutionalised in any future mechanism.
- Make space for the technical community. This community makes not only attribution possible, but other cyber security assurances too. As well, the PoA should bear in the mind the cadence of what regional organisations are already doing—how can meetings of regional organisations facilitate aspects of what the PoA eventually includes, for example.
- Remember that the participation of the technical community and industry is a "two-way street." This community can provide insights on new threats and techniques, but it can also gain information from these conversations about how technology is being used and misused in different contexts around the world.

CONFIDENCE-BUILDING MEASURES (CBMs)

10 December 2020
SESSION REPORT

GENERAL SUMMARY
13:00 UTC
Co-chairs

- Hungary
- Chile
- Derechos Digitales

The session attracted a broad participation of 148 people who joined the event from Zoom and the Livecast. The Livecast attracted viewers from 15 countries and 20 cities around the world.

SESSION OUTLINE

The session opened with an introduction by the moderator Mila Francisco of Chile, who summarised the rules of the discussion as well as the central themes of the session, introducing the main questions and topics for the session:

- *How do regional organizations approach the development in implementation of CBMs at the regional level? What are the fundamental similarities and differences?*
- *What did the Organisation for Security and Co-operation in Europe (OSCE) and the Organisation of American States (OAS) deliver in terms of CBM implementation and cross-regional information exchanges? Views of non-governmental stakeholders.*
- *With respect to the draft "CBM" section of the OEWG pre-draft report (points 45-52), are there any notable omissions, or statements with which you disagree? The role of non-state actors, NGOs, tech companies, etc. in the implementation of CBMs, the outreach activity of international organizations towards them.*

Péter Tamás Horváth of Hungary started the presentations, providing some scene-setting and highlighting the main activities of participating states at the OSCE in developing and implementing CBMs. The informal working group on cyber issues of the OSCE was established to develop consensus on CBMs, to enhance cooperation, transparency, predictability and stability in state relations, and reduce the risk of escalation and misperception, continuing the successful work on CBMs for conventional conflict. OSCE's CBMs call for responsible state behaviour in the use of ICTs, dealing with transparency, communication, and national preparedness to address cyber challenges. Multi-stakeholder participation is encouraged at the OSCE, with key events gathering diverse non-governmental

stakeholders. The OSCE is also a testing ground for new ideas, such as the "Adopt a CBM" initiative.

Szilvia Toth, from the OSCE Secretariat, reinforced the history of the OSCE creating instances for cooperation around confidence-building measures, as well as cooperation with regional organisations. Emphasis is placed on implementing CBMs. Although the OSCE engages in cyber issues in a working group with government representatives, other stakeholders are regularly invited to present on topics related to on CBMs implementation. Efforts include workshops and trainings, involving non-governmental stakeholders, which allows a wider perspective and exchange with government representatives. OSCE CBMs encourage participating states to engage with stakeholders and national structures.

Pablo Castro, from Chile, emphasised the history at the OAS of confidence and security building measures as an important tool promoting peace, building trust and enhancing cooperation. A natural step forward in this historical process is the creation of CBMs in cyberspace, and Inter-American dialogue allowed for a common cybersecurity strategy. The OAS working group on cooperation and CBMs in cyberspace was established with the mandate to draft CBMs based on the consensus UN GGE 2015 report, with recommendations that have included providing information on cybersecurity policy; designating national points of contact at the policy level; and strengthening and promoting cyber diplomacy. The latter responds to a need of engagement of Foreign Affairs Ministries in cyber discussions. Challenges remain on implementation, linkage to other issues such as norm implementation and the application of international law, and gender considerations in cyber policy. Non-governmental stakeholders are engaged at the OAS level, and can play different, important roles at the national and international levels. Lessons can be gathered from other regional organisations as well.

Louise Marie Hurel, from Igarapé Institute first provided an overview of the changing and expanding nature of CBMs, looking at them broadly in the context of a changing discussion on CBMs from conventional conflict to cyberspace, and highlighting the cross-pollination happening between different initiatives; also, a shift in focus from the context of traditional disarmament and arms control, with questions of peace and stability seen through the challenges of cyberspace, and the difficulty to separate the national/regional/international levels. Focus was brought to the convergence between confidence, cooperation and coordination**.** Non-governmental stakeholder engagement requires not only attending discussions, but working together at the national and regional level, bridging the gaps between different kinds of knowledge, and consolidating views. Non-state actors can help in specific elements: ensuring there is a rights-respecting and gender-sensitive lens in the formulation or implementation of CBMs and enhancing capacities for implementation of the CBMs. Good practices can be improved too, for instance, to consolidate points of contact designated for specific agendas, like critical infrastructure, cybercrime, etcetera, to flesh out different dimensions of CBM implementation.

Finally, Andraz Kastelic, from UNIDIR, presented the Cyber Policy Portal: a confidence building tool developed in 2019, as an interactive online tool providing information on

cybersecurity policy by UN member states. As such, it promotes transparency and facilitates information exchange and capacity; by doing so it attempts to dispel ambiguities and reduce tensions among nations in cyberspace. It is aimed at diplomats, policymakers, and security policy experts.

The interventions were followed by an open discussion. Participants and panellists discussed the role and the value of CBMs in practice, their importance in the context of attribution of cyber incidents, and good practices in communication between different stakeholders such as diplomats and CSIRTs. Closing remarks by J. Carlos Lara of Derechos Digitales emphasised takeaways regarding effectiveness of CBMs, the need for inclusiveness in their development and evaluation, and the need for further discussion and encouragement in international forums, including in the context of the OEWG.

MAJOR THEMES / AREAS OF CONVERGENCE

- *Implementation as the priority challenge.* Implementation remains a common challenge, and though there seems to be a lack of appetite to develop new CBMs, there seems to be consensus that meaningful implementation of known CBMs is crucial. There needs to be a more honest conversation between state representatives on how to implement already recommended CBMs.
- *Regional organisations play an important role in norms implementation.* Regional organisations have manifested their intention to develop and implement CBMs as a major driving force for multi-level efforts to build trust among states and non-state actors. Regional organisations play an important role in translating CBMs into practice, including through information exchange, capacity building, and gathering of best practices. At the same time, dialogue between different regional organisations, as well as complementary dialogue at the global level, can support CBM adoption.
- *Following up is a key element of implementation.* CBMs allow the conditions for principles, rules and norms to function in practice. But to understand whether they can serve their purpose in the event of an attack or crisis related to ICTs, their implementation must be monitored and independently evaluated. Otherwise, cooperation and procedures to deal with cybersecurity crises can fall short on their promises to generate trust and prevent escalation in case of incidents.
- *CBMs are complementary to other efforts, especially capacity building.* CBM implementation goes hand in hand with capacity building. Capacity building also creates buy-in and ownership from participating states and allows for meaningful discussion of CBMs between state representatives. It ensures that what ministers agree in meetings is translated into action, making sure countries have capacities and resources to maintain commitment to implement CBMs, and incorporating rights-respecting and gender-sensitive perspectives.
- *Taking stock of existing CBMs*. Confidence building measures have been highlighted and reported before, but there is a need to map these mechanisms because states and non-state actors need to know what is available and what is already in place, ensuring that there is no

overlap of mechanisms, that the mechanisms and channels that are available are used, and that there is interpersonal trust at different levels. Good practices such the informal daily communications between CSIRTs, also represent trust-building activities that need to be highlighted.

- *The role of non-state actors.* In different national and regional initiatives, non-governmental stakeholders are actively involved in the discussions on how to implement CBMs. Non-governmental stakeholders can play key roles in capacity building, as well as in the design, implementation, monitoring and evaluation of CBMs.
- *The impact of building trust.* The repercussions of large-scale cyberattacks affect states, but also individuals and other sectors. Trust is transversal and requires an approach that considers the impact of cyberattacks in the implementation of CBMs. Trust must be built also with all possibly affected individuals and groups as well.

RECOMMENDATIONS

- States and international and regional organisations should maintain and build upon efforts for implementation of existing confidence-building measures. States should also consider monitoring and evaluation mechanisms to follow up implementation.
- States and international and regional organisations should maintain and build upon regular information exchange as a confidence-building mechanism, utilising the forums already in place and engaging with different stakeholders. States should endeavour to map and learn about measures that are already present in other countries and regions, as well as the best current practices of non-governmental stakeholders.
- States should prioritise mechanisms to support implementation of known confidence-building measures involving non-governmental stakeholders.
- States and regional organisations should endeavour to engage in more inter-regional dialogue for all CBM processes, not just on cyberspace, to prevent escalation of conflicts. States should accordingly clarify the roles and expertise of different representatives, while allowing meaningful dialogue between different forms of expertise.
- The OEWG report should include reference to the role of non-governmental stakeholders, including civil society, academia, the technical community and industry, in supporting the implementation of norms, rules and principles. The OEWG report can be expanded with a reference to CBMs developed by States that require the involvement of the private sector to be fully operationalised.
- Existing mechanisms that involve non-state actors should be expanded to include stakeholders currently not participating in discussions, in order to improve states' capacity to integrate different rights-respecting perspectives in the adoption of measures to build trust with other states as well as other stakeholders.

[SIDE EVENT] GENDER APPROACHES to CYBERSECURITY

09 December 2020
SIDE EVENT REPORT

GENERAL SUMMARY
13:00 UTC
Co-chairs

- Women's International League for Peace and Freedom (WILPF)
- UNIDIR
- Canada
- Chile

As part of the Informal Multi-Stakeholder Cyber Dialogue, the *Gender Approaches to Cybersecurity* side event aimed to help shed light on the numerous initiatives relating to gender and cybersecurity. There were 185 participants who joined the event from Zoom and the Livecast including government representatives, non-governmental organisations, academia, and private sector stakeholders. The Livecast attracted viewers from 16 countries and 23 cities around the world.

SESSION OUTLINE
Allison Pytlak, Programme Manager at the Women's International League for Peace and Freedom (WILPF) moderated the session. Sirine Hijal, Deputy Cyber Foreign Policy Coordinator, Global Affairs Canada opened the event by highlighting three achievements related to incorporating gender approaches in international cybersecurity discussions. These include:

- Increasing support from many States for addressing gender issues at the UN Open Ended Working Group (OEWG).
- Research funded by Canada on gender and cyber (available on the OEWG portal here and here) which has led to more research efforts, providing better data and better analysis to inform the OEWG's work.
- Thanks to the *Women in Cyber Fellowship Program*, the OEWG achieved equal participation of women in its in-person meetings, which is a first for a First Committee-based process.

Collectively, these achievements have built a base of future experts who can mentor others and show the possibility those women have in contributing meaningfully to cybersecurity negotiations.

Ambassador Jürg Lauber, Permanent Representative of Switzerland to the United Nations, also shared his experience as OEWG Chair and involvement in other UN processes, including in his role as an International Gender Champion. Amb. Lauber drew two important lessons from these efforts:

- *The importance of diversity*: where diverse perspectives and experiences can enrich international discussions, and this can also ensure that we propose the best solutions to address the common challenges we face.
- *Representation of women*: women remain underrepresented in multilateral negotiations, even if there have been efforts to promote the participation of women through initiatives such as the International Gender Champions (IGC).

UN Institute for Disarmament Research (UNIDIR) Consultants Kate Millar and James Shires then presented their forthcoming research on the interconnections between gender norms and the field of cybersecurity. Dr Millar highlighted the difficulty in identifying the connections between gender norms and cybersecurity, as both are highly abstract concepts.

Dr. Millar also explained that gender informs cybersecurity in two ways: first, gender norms can construct individual roles, identities and expectations about behaviours in the cyberspace; second, we can also think about how gender operates as a hierarchical social structure. Dr. Shires further explained that there are three ways through which cybersecurity standards can become, first, more gender-sensitive and then ideally, more gender-responsive:

- Meaningful participation in the development and consultation around the creation of standards.
- The language and content of standards need to be examined from a gender perspective.
- Measuring the impacts of the standards based on disaggregated data collection.

Next, Paloma Herrera, researcher and coordinator of the gender and cybersecurity course at the University of Chile, also complemented UNIDIR's research findings, but from a cybersecurity policy level. She looked in particular at the main objectives of Chile's National Cybersecurity Policy, which strives to improve the security of standards in cyberspace and to ensure the full enjoyment of fundamental rights for people in equal conditions. She stressed that to achieve this objective, multilateral cooperation is essential.

Finally, there was a short presentation by Mila Francisco, diplomat at the International and Human Security Division in the Ministry of Foreign Affairs of Chile in Santiago and an active participant in the *Women in Cyber Fellowship Program*. She shared her personal experience as a fellow and discussed the impact of the programme on the OEWG process. She sees the fellowship programme as a driving force for encouraging female government representatives in the OEWG, and in building a strong peer network among its participants. After the moderated discussion amongst the speakers, the moderator opened to floor to questions and comments, including interventions from participants on the Zoom call and livestream chat. Some of the main themes of these discussions are captured below.

MAJOR THEMES / AREAS OF CONVERGENCE

The side event on *Gender Approaches to Cybersecurity* offered an opportunity for both State representatives and non-governmental stakeholders to further explore the inclusion of gender in cyber security and how this issue can be addressed at the OEWG and in other processes. As such, women's and gender diverse participation and representation was a major theme throughout. Some suggestions made in this regard by participants in the Q&A included:

gender mainstreaming; the value of gender literacy and knowledge; and finally, it was noted that addressing gender equality and feminist concerns can and should become a regular feature of international cybersecurity discussions. One participant asked about how to increase gender diversity among non-governmental OEWG participants as well, and another highlighted that there are also many regional and local groups of women that work in cyber whose perspectives could be leveraged to strengthen UN discussions.

The use of data was also highlighted as an important factor in supporting the work of promoting gender inclusion. It was stressed that by using data, we can improve interventions and support the practice that women are amplifying each other's voices in discussions. Even though current data available on this issue is limited, there may be data available about other processes which can be leveraged and supported in cyber processes. Finally, it was recognized that the participation of male allies and gender champions at the top of cyber organizations, the UN and foreign ministries is also necessary to make progress on these issues.

Beyond the above themes, the side event discussion highlighted areas for further work or research. This includes questions around how to broaden discussions of what constitutes 'expertise' and how to overcome gender-blindness within the technology sector and in government; and how to also improve awareness about potential gendered impacts of cyber operations, or gender biased algorithms. One participant noted that the term "gender" has become weaponised in online spaces and used as a mobilising tool by non-state actors, while another participant pointed to the importance of going beyond numbers alone, given that state representatives of any sex or gender are still bound by the instructions they receive from their governments, and that the formulation of security policy is often 'male-centred'.

NEXT STEPS

In terms of next steps, UNIDIR promised to share the research report authored by Dr. Millar and Dr. Shires on gender and cyber in January, when it is finalized. In the meantime, a commentary from them is available on the UNIDIR website. Canada will keep working with other States who are interested in addressing gender issues by promoting text to address gender in the OEWG report, including the gender text proposals that are included in Canada's broader OEWG text proposals. Dr. Herrera and other Chilean researchers will continue sharing their research on gender and cyber as well, building on the papers that were already uploaded to the gender section of the event series site.