Canada's response to questions in Chair's paper: February 2020 OEWG meeting

Threats

Are there any existing or potential threats that have not been mentioned in the First substantive session that should be discussed (or require further discussion) in the OEWG?

- Previous GGE reports made some useful descriptions of the ICT threat environment. However, the ICT threat landscape is fast evolving.
- It would therefore be a useful exercise to update our common understanding of the threats we face today, so we are able to better address them collectively.
- In so doing, we should be mindful that the OEWG is a body of the First Committee, and the focus of its work should thus be on describing cyber threats that could affect international peace and security. This could include the risk of miscalculation and escalation of tensions when there are cyber incidents between States.
- It could also be useful to briefly discuss potential future cyber threats, such as the growth of the Internet of Things, artificial intelligence, supply chains and quantum computing, that might affect the threat landscape and relations between States in the coming years.
- In our view, it would not be productive to address threats such as terrorist use of the Internet or cybercrime, which do not fall under the OEWG's mandate.
- These issues are being addressed in other fora and elsewhere in the UN system, including UNGA's Third Committee and the UN Security Council's Counter-Terrorism Committee. The OEWG should not create confusion by duplicating these efforts taking place elsewhere.

International law

Which, if any, are the gaps in international law?

- Canada believes that existing international law and the agreed UN GGE norms of State behaviour are sufficient to guide State's behaviour in cyberspace.

What would be the appropriate format(s) to address possible gaps in international law?
-legally binding treaty
- politically-binding agreements
- guidance notes fostering common understanding of existing international law
- other

- Canada continues to believe that existing international law and norms developed by the GGE (in its 2013 and 2015 reports) and by the G20 (the "no ICT-enabled theft of intellectual property for commercial gain" norm) are explicit and largely sufficient to guide State behaviour.
- We believe that the proposal to develop a treaty or binding instrument on cyber issues would undermine existing international law and the GGE norms.
- Also, we should keep in mind that the 2016-17 GGE failed to reach consensus, largely because of some divergence in views over how international law applies in cyberspace.
- It is worth underlining that States do not challenge the application of international law to cyberspace as such, but have differing views on *how* the law applies. This is not surprising, given the rapid developments in cyberspace.

- This issue is best addressed through the continued development and public articulation of national positions and capacity building to support this, so that all States can expand their understanding of international law as it applies to cyberspace, through continued dialogue.
- To avoid a repeat of the 2016-17 GGE outcome at the upcoming OEWG, we think the OEWG should minimize discussions on the details of how international law applies in cyberspace. Trying to identify gaps in international law is likely to cause divisions rather than help us achieve consensus.
- Instead, Canada believes the OEWG could usefully consider and make recommendations to expand capacity building activities, so that more States can advance in their national understanding, the development of their national positions, and engage more fully in dialogue, which will help expand our common understanding.
- The issue of how international law applies in cyberspace will be addressed at the GGE, via the Annexes that GGE States are being asked to submit on how they see international law applying in cyberspace.
- Non-GGE States can submit their views on this issue in their annual submissions to the UN and elsewhere. This is what Canada plans on doing, likely as part of our 2020 annual submission to the UN.
- In terms of what to include in an OEWG report, the group could simply reiterate the conclusion of the 2013 and 2015 GGEs that international law applies in cyberspace. Consensus on that point should be reached without difficulty. This could be followed by discussions on the shared understanding of the benefits of capacity building of national expertise in international law as it relates to cyber activities. Doing this would be of interest to a wide range of States, and could be included in the report both as a point of convergence and as a recommendation.

Is there a gap in capacity building on international law that the OEWG could address?

- Canada believes that expanding capacity building on international law as it applies to cyberspace is an important topic that the OEWG could usefully address. We heard support for this from a range of States at the February session and in various bilateral discussions.
- Several States have acknowledged not being as familiar as they would like with how international law applies in cyberspace. To address this knowledge gap, States that have devoted more thought to how international law applies in cyberspace could be encouraged to offer capacity building support that responds to the needs of particular States.
- This could begin with workshops on law and norms on request by States seeking support. Other forms of capacity building assistance could also be offered to improve the latter's knowledge of these issues, including online training and virtual workshops for diplomats and officials who work on these issues. This knowledge could then be consolidated and validated in simulations or tabletop exercises at national, sub-regional and regional levels.
- Canada and other States have already organized workshops along these lines. Additional efforts such as these should be encouraged.

Should there be a central repository of national practice in the application of international law?

- The resolution that created the GGE recommends that States make submissions via Annexes to outline their views on how international law applies in cyberspace. GGE member States could use these to share their positions and practice. Non-GGE States can submit their views on this issue in their annual submissions to the UN or elsewhere.

- We would be open to exploring the possibility of creating a central repository of national positions in the application of international law, submitted by the respective State. We would have to determine who would create and maintain such a repository and some other issues, such as parameters for submissions.

Norms

Should the OEWG recommend ways to raise awareness of existing norms and commitments? If so, what should those be?

- Canada has endorsed the norms adopted by previous GGEs and is actively working to promote their implementation.
- Canada and Australia have posted submissions on the OEWG portal that describe how we have implemented the norms adopted by past GGEs.
- Other States that have already implemented the GGE norms should consider posting similar submissions, in order to provide examples to developing States and States who are less familiar with the GGE norms of the types of actions that they can take to implement those norms.
- Regional organizations have also done excellent work on raising awareness of norms. This type of work should continue.
- Capacity building efforts should also be undertaken to promote awareness of GGE norms.
- Canada is building capacity of cyber diplomats by organizing workshops to help States better understand the outcomes of GGE reports and what can be done to implement them. For example, we co-hosted a workshop with Mexico and the OAS in May 2019 that targeted OAS States. We organized another similar one targeting Francophonie States in September 2019.
- We have found that these types of workshops are an excellent way to raise awareness of existing norms.
- Canada is also funding the participation of female diplomats from the Americas at OEWG meetings, as part of the Women in Cyber fellowship program. This fellowship program is promoting the meaningful participation of women in UN cyber discussions. We hope that it will also help the Group develop a better understanding of the gender elements of cyber security.

Should the OEWG recommend ways to improve operationalization of existing norms? If so, what should those be (for example, implementation roadmaps)?

- Norms have to be widely known and implemented to be effective, and the OEWG should help strengthen their successful and sustained application by States.
- Canada therefore believes that an eventual OEWG report could provide concrete guidance on norm implementation. The OEWG report could explain what each of the General Assembly endorsed norms means in practice, and give concrete advice on how they could be implemented by States and regional organizations.
- The guidance on norm implementation included in the draft 2016-17 GGE report could serve as a model for the OEWG's work. In that draft report, which was never adopted because of lack of consensus over other issues, each of the 11 norms from the 2015 GGE report was explained, and guidance on their implementation by States and regional organizations was provided.
- The OEWG could aim to provide similar guidance on norms implementation in its report.
- This work would have to be coordinated closely with the GGE's work on norms, to avoid any duplication or contradiction.

- Regional organizations have also done excellent work on promoting the implementation of existing norms. This type of work should better disseminated so that all States are aware of best practices and successful initiatives. States and regional organizations should also encouraged to help build capacity where needed.
- Once the GGE and OEWG adopt their final reports, the OEWG and GGE Chairs and UNODA officials should work closely with regional organizations to promote the operationalization of the norms adopted in previous GGE reports, as well as any additional guidance on norms implementation that might be agreed on by the current GGE and/or OEWG.
- The idea of implementation roadmaps is an interesting one that the OEWG and/or GGE could examine as well, but these types of roadmaps should be tailored to each State's or region's individual circumstances and capacity.
- Some models already exist, like the Cybersecurity Capacity Maturity Model for Nations. These models have been extremely useful for partners in developing the most effective cyber capacity building projects for regions or countries.
- They provide an initial foundation based on previous experiences and actual needs of specific regions or countries. These types of roadmaps can be a useful way to share expertise, avoid duplication and avoid having to do assessment missions for each project.
- Gender should be taken into account in the operationalisation of existing norms, and the OEWG could provide guidance to States in this regard.

Is there need at this time for additional norms for responsible State behaviour on issues such as:

- supply chain neutrality
- attribution
- non-interference in internal matters (such as political processes)
- prevention of escalation
- media/private sector responsibility
- protection of the public core of the Internet
- or others

- From Canada's perspective, existing norms developed at the GGE (in its 2013 and 2015 reports) and by the G20 (the "no ICT-enabled theft of intellectual property for commercial gain" norm) are explicit and largely sufficient to guide State behaviour.
- At this stage, we do not believe that new norms are needed, as most of what is being proposed is already covered either by existing international law or norms.
- Rather, we believe that States should focus on implementing existing norms.
- Many States and observers have argued that the current norms are not widely observed. Our efforts should therefore focus on increasing respect for current undertakings.
- We should also focus on how the international community can better support States' ability to develop the capacities needed to implement and operationalise these norms.

Should Member States unilaterally declare to refrain from militarization/offensive use of ICTs?

- Canada recognizes cyberspace as a domain of military operations, as does NATO, its member States, Australia and a number of other countries.

- From Canada's perspective, offensive ICT capacities are not necessarily bad in and of themselves. They are a military capability like any other, subject to the same rules as other military capabilities. There are entirely appropriate uses for these capabilities.
- Several States, including Canada, have declared offensive cyber capabilities. Some States have also publicised the legal frameworks that govern their possible use. Canada supports this approach and plans to share our positions on the applicable law in the coming months.
- In Canada's view, a realistic objective is to promote transparency. This means encouraging States to be open about their capabilities, and the conditions under which they would use them. Another realistic and constructive objective is ensuring that States follow international law and agreed norms if they use their offensive cyber capabilities.
- Canada's Defence Policy, released on June 7, 2017, recognized the growing threat posed by malicious actors in cyberspace. To help protect and defend Canada, our Defence Policy stated that the Canadian Armed Forces are developing the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions. It also specified that all our missions are subject to all applicable domestic and international law.
- Canada is being very candid and transparent about our cyber capabilities. We are also being very clear that these capabilities would only be used in a manner consistent with our international legal obligations and with agreed norms of State behaviour.
- Several other partners and allies have been similarly transparent about their capabilities and the conditions under which they might be used.
- In Canada's view, it is essential that States be transparent about their intentions, including by committing to only using their capabilities in accordance with their international law obligations and in respect of agreed norms. Doing so would help to address the threat of misperception, miscalculation and escalation.
- Canada therefore encourages other States who possess offensive cyber capabilities to be transparent about their existence, and to pledge to use them in accordance with international law and existing agreed norms of State behaviour.

Could the OEWG usefully further elaborate on the linkages between norms, confidence-building and capacity building measures?

- Yes, that could be a useful role for the OEWG. The OEWG report could provide advice on how to use capacity building and CBMs as a means to implement existing norms and promote compliance with international law.
- For example, several States have indicated that the main barrier to norms implementation is lack of capacity. Other States have indicated that they are not as familiar as they would like with how international law applies in cyberspace. To address these knowledge gaps, States with more experience on issues related to international law and cyber norms could be encouraged to offer capacity building support that responds to the needs of particular States.
- The OEWG could provide additional insights on the linkages between norms, CBMs and capacity building, as well as offer concrete suggestions as to how CBMs and capacity building can be used to promote greater understanding and implementation of existing agreed norms.
- The OEWG should take advantage of existing cyber capacity building coordination bodies such as the Global Forum for Cyber Expertise (GFCE), in order to maintain coordination and coherence as it relates to cyber capacity building efforts.
- The GFCE regularly produces roadmaps and publications on how to improve cyber capacity building efforts and develop CBMs and standards.

- More importantly, with the launch of the GFCE Foundation, they will be able to start acting as a capacity building hub. This means that countries will be able to highlight their capacity building needs and propose projects to meet these needs.
- These proposals can then be assessed against other research and expertise in order to begin conversations with recipient countries. This will in turn hopefully allow countries to develop the most effective capacity building projects possible.
- It will be important for recipient nations to include opposition parties in the development of cyber capacity building projects and the establishment of CBMs, in order to ensure their sustainability. The GFCE can work as a hub to facilitate this type of coordination.
- The OEWG should continue to participate in GFCE bi-annual meetings, in order to maintain a clear line of communication and coordination between cyber capacity building partners and the OEWG. This would also allow the OEWG to have a direct platform to provide regular recommendations on how to better coordinate and structure capacity building initiatives.

CBMs

Are there regionally developed confidence-building measures that are ready to be recognized on a global level?

- Regional organizations have had more success implementing certain CBMs than others. Some of these CBMs could be ready to be recognized on a global level.
- Canada has been working on CBM implementation with several regional organizations. For example, Canadian initiatives at the OSCE have included:
    - championing CBM 4 (promote information sharing on national approaches to ensure an open, secure, interoperable Internet);
    - supporting workshops on international law and cyber operations;
    - co-hosting a scenario-based discussion on CBM 5 (sharing information about national responses to regional cyber incidents).
- At the ARF, Canada co-hosted a workshop with Singapore in the spring of 2019 on the principles of building cyber security in the national context.
- The OAS has also done useful work on CBM implementation that Canada has contributed to. For example, it has built a list of points of contact, and it has established a repository of cyber related policy and legislation.
- In May 2019, Canada also teamed up with the OAS to host a workshop on cyber diplomacy for diplomats from OAS countries who work on cyber files.
- These are only a few examples of the great work that regional organizations have done on CBM implementation, and Canada looks forward to continuing to take part in this important work.
- Regional organizations could be asked to provide a list of the CBMs from previous GGE reports that they have had the most success in implementing. The CBMs that are identified by most or all regional organizations could then be identified and prioritized for implementation by all States.
- To facilitate this work, regional organizations such as OAS, OSCE, AU, ASEAN should be proactively included in our work.

Are there any new confidence-building measures that the OEWG should consider recommending?

- Regional organizations such as the ARF, OAS and OSCE have done excellent work on developing and implementing CBMs.

- For example, regional organizations such as the OSCE have established CBMs to encourage support and information sharing on incidents.
- Canada has been proud to support the work of regional organizations in implementing CBMs. For example, at the OSCE, we are championing CBM 4, which aims to promote information sharing on national approaches to ensure an open, secure, interoperable Internet.
- In September 2019, Canada also teamed up with the Francophonie to organize a workshop on international law. This workshop allowed diplomats from Francophonie countries who work on cyber files to better understand how international law applies in cyberspace.
- Despite this progress, some States and regional organizations have indicated that they face challenges and barriers in the implementation of the CBMs recommended by the 2013 and 2015 GGEs.
- Rather than attempting to develop new CBMs, Canada hopes that the OEWG will focus on practical measures to apply and implement the voluntary CBMs and transparency measures adopted in the last two consensus GGE reports.
- While previous GGE reports laid out CBMs, they provided limited guidance on how the CBMs that were developed by the GGE could be translated into concrete State action.
- There may be a role for the OEWG in providing guidance in this regard by proposing practical measures to disseminate, apply, and implement existing CBMs, including their gender dimensions.
- The OEWG report could also examine avenues for cooperation in regional forums and other groupings, with a view to determining the most productive way to advance the development and promotion of CBMs in these forums over the coming years.
- Ensuring more meaningful participation of women in international cyber negotiations is another way to help build confidence, in Canada's view.

Is there a need to establish a global repository of existing confidence-building efforts at regional and sub-regional levels?

- While there could be value in establishing such a repository, a question that would need to be answered is who would establish and update such a list.
- It would perhaps be more fruitful to promote an increase of inter-regional collaboration and discussion.
- For example, the OSCE has started an inter-regional exchange with ASEAN on CBMs. Once a year, OSCE cyber working group participants go to ASEAN to present what has worked and what has not worked as well when implementing CBMs. This has been a very useful venue to facilitate conversations on best practices related to CBMs. This model could perhaps be emulated by other regional organizations.

Is there a need to establish a global list of Points of Contact?

- There is already a global points of contact list of national CSIRTs and CERTs hosted by the Software Engineering Institute at Carnegie Mellon University.
- The European Union Agency for Cybersecurity (ENISA) also maintains a list of European CSIRTs.
- This means that global points of contact lists already exists. Rather than creating a new global list, national CSIRTs could be encouraged to list themselves on the SEI website, as Canada has done.
- Several regional organizations, such as the ARF and OAS, already have points of contact lists as well. For example, Canada has participated in several OSCE exercises that used the points of contact CBM

to share information among participating States' points of contact (at both the technical and policy level) during simulated cyber crises.

- During a real cyber incident, these contacts could be used to defuse real crises by allowing CERTS, Interior and Foreign Ministries and relevant technical points of contact to communicate rapidly.
- The OSCE has had some successes in bringing Points of Contact together to discuss national approaches to addressing cyber incidents through scenario-based discussions and workshops, as well as by increasing the face-to-face contact with our direct counterparts.
- This highlights the need to go beyond just having a Points of Contact list, but also of having exercises to test how the list would be used in times of crisis.

Capacity building

How can capacity building be best coordinated on a global level?

- Cyber Capacity building can be better coordinated through international capacity building organizations such as the Global Forum for Cyber Expertise (GFCE). The GFCE offers a platform for States, international organizations and private companies to exchange best practices and expertise on cyber capacity building, with the aim of identifying successful policies, practices and ideas in order to multiply them on a global level.
- Together with partners from NGOs, the tech community and academia, GFCE members are able to develop practical initiatives to build cyber capacity. The GFCE has made significant progress since its establishment to increase participation and provide all participants with the tools, knowledge and expertise required to coordinate global efforts in cyber capacity building. Though there is still work to be done in order for the forum to reach its full potential, Canada believes the GFCE is best placed to manage this coordination globally.

Are there principles of capacity building which the OEWG could recommend?

- There are several important principles that the OEWG could recommend that States follow when it comes to capacity building.
- Canada believes that member States must make cyber security capacity development a priority at the highest level. Unfortunately, some States still place a low level of priority or allocate relatively few resources to these efforts.
- This has been particularly the case in relation to the establishment of career paths for incident response professionals. For instance, many States do not have a national CSIRT, and many of those that have one do not provide it with adequate human or financial resources.
- In some States, there is a need to speed up to process of improving legislative frameworks, which will facilitate greater cooperation among States for investigation and knowledge sharing. These legislative frameworks should also include incentive schemes and financial structures that would allow the incubation of new businesses and the recruitment of new talent into their economy and cybersecurity supply chains.
- It is important to coordinate efforts in cyber capacity building, both regionally and within individual States. Certain projects have faced issues related to programming overlap, as donor nations sometimes seek to showcase to their own governments how they are addressing the main cyber concerns individually, rather than collaboratively.

- As a result of these missed opportunities to approach capacity building gaps in regions or States collectively, there have been signs of programming overlap, where the same issue is being addressed by two different donors.
- It is therefore important to analyze and assess the capacity building needs collaboratively and agree on a collective approach. Implementing organizations must also be conscious of this, as they are more directly involved on the ground. These organizations need to show more of a willingness and initiative in proposing projects that clearly outline how they will be integrating their efforts into a larger regional or State-specific approach.
- Donors and implementing partners need to do much more work engaging civil society and academia, especially when it comes to the development of national strategies. This issue has consistently been left out of the conversation in many States. This is of particular importance as activities such as these are a key area in which gender equality and human rights can be fully integrated into these policies.
- It is important to carry out gender-based analysis in the development of capacity-building programs, and to take measures to ensure the meaningful participation of women in program-related activities.
- Furthermore, even though gender equality objectives may be integrated in these strategies, if civil society organizations active in these areas are not properly engaged throughout the process, the real concerns or driving factors creating inequality will not be properly represented or understood, which in turn results in strategies that are not truly effective at addressing these issues.

What relevant lessons might be drawn from other matchmaking initiatives under UN auspices that could inform the necessity, practicality and utility of establishing a new mechanism?

- Canadian programmers have worked with a number of UN organizations, and the experience has been wide ranging. For the most part, we have found that the UN works well at clearly defining each organization's mandate in order to tailor collaborative approaches to capacity building needs.
- In some cases, UN organizations have been able to function as a key coordinating hub that is capable of tracking projects in the region, identifying threats and capacity building needs, as well as sharing these insights with partners.
- Canada believes that a new UN mechanism to coordinate cyber capacity building needs is not necessary at this time.

<u>Institutional dialogue</u>

How should a new regular institutional dialogue under UN auspices be constructed in terms of:

- purpose
- scope
- participation (including role of non-State actors)
- frequency
- financing
- other

- Canada hopes that any successor mechanism to the OEWG will not create any new formal structures or bureaucracies that would take away from the important work and resources needed to reinforce the capacity of UN member States.

- We have agreed that the consensus rule will apply to the OEWG's work, and we believe that an eventual successor process should also apply this rule.
- We hope that a successor process will also include a mechanism to gather civil society and private sector input, in order to ensure that a broad range of views continues to be represented in any successor process.

How could regular institutional dialogue on ICTs and international security best be coordinated with ICT-related discussions at the United Nations on other topics (such as crime, development, human rights, etc.)?

- In developing a successor mechanism or institutional dialogue, we should be mindful that the OEWG is a body of the First Committee. The focus of its work should thus be on addressing cyber issues that could affect international peace and security, as well as proposing means of promoting peace in cyberspace, such as norms of State behaviour and CBMs.
- If there is no consensus at the OEWG on certain issues, an eventual successor mechanism or institutional dialogue could continue deepening States' mutual understanding of issues on which there is disagreement, such as how international law applies in cyberspace.
- We should also be mindful that the UN has limited budgets to address cyber issues, so it may not be possible to create new UN structures or mechanisms to address these issues.
- In Canada's view, form follows function. We should determine what a successor mechanism wants to achieve, and then discuss what form this mechanism should take to best achieve its objectives.
- It will be important for any successor mechanism to coordinate closely with the cyber-related work taking place in other fora and elsewhere in the UN system, whether it be the work underway at UNGA's Third Committee, the UN Security Council's Counter-Terrorism Committee or the Internet Governance Forum.

Should there be additional formats for multi-stakeholder dialogue?

- We are pleased with the degree of multistakeholder participation in the OEWG's work to date, especially with the fact that all stakeholders were invited to the December 2019 multistakeholder consultation, not just those on the ECOSOC list.
- We hope that they are able to continue to share their views on the OEWG process and that their input is meaningfully reflected in an eventual OEWG report.
- There are already various other forums for multistakeholder dialogue, so we do not believe that any additional ones are necessary at this time.
- We hope that an eventual successor process will also include a mechanism to gather civil society and private sector input, in order to ensure that a broad range of views continues to be represented.