
Summary

This paper outlines the issues that Canada would like to see addressed at the 2019-20 Open-Ended Working Group (OEWG), in a manner that builds on the acquis of the 2013 and 2015 consensus reports of the UN Group of Governmental Experts (GGE) on “Developments in the Field of Information and Telecommunications in the Context of International Security.” Canada proposes that the 2019-20 OEWG focus on practical measures to apply and implement the voluntary norms of State behaviour, confidence-building measures (CBMs) and transparency measures adopted in the last two consensus GGE reports. With respect to cyber capacity building, Canada believes that the OEWG report could help promote cooperation in order to expand and better prioritize capacity building resources. Given the broader scope of the OEWG, and the participation of a wide variety of actors in this process, Canada hopes that the OEWG will be as inclusive as possible and that its report will address issues such as defending online freedoms and promoting gender equality. The rationale for this proposed approach and more specific examples of what could be included in the OEWG report are outlined below.

Background

The 2013 GGE report affirmed the applicability of international law to State behaviour in cyberspace. The 2015 report of the GGE was adopted by consensus in resolution 70/237, which “calls upon Member States to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts.” It set out the following voluntary, non-binding, peacetime norms of State behaviour in cyberspace, among others:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.
- States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.

Canada sees the applicability of existing international law to State behaviour in cyberspace, together with the implementation of these norms, as the foundation of sustaining international peace and security through the promotion of responsible State behaviour in cyberspace. That is why Canada strongly supported the adoption of these norms and continues to promote their endorsement and implementation in various forums (including the G7, G20, North American Leaders’ Summit, NATO,
ASEAN Regional Forum and OSCE). The 2015 GGE report also encouraged the development of transparency measures and CBMs, which Canada has supported as well.

Canada believes that an eventual OEWG report could provide concrete guidance on norm implementation. The OEWG report could explain what the norms mean in practice, and give concrete advice on how they could be implemented by States and regional organizations. Canada reiterates the conclusions of the 2013 and 2015 GGE reports and looks forward to supporting the implementation of the GGE’s previous, successful outcomes in the coming year at the OEWG.

Scope of issues to be addressed at OEWG

Canada’s view is that the OEWG should take a pragmatic and realistic approach to its work in order to ensure that it yields concrete results. While previous GGE reports recognized that international law applies in cyberspace and laid out norms and CBMs, they provided limited guidance on how the norms and CBMs that were developed by the GGE could be translated into concrete State action. That is why we believe that the OEWG focus should now be on proposing practical measures to disseminate, apply, and implement existing agreed norms and CBMs. Norms have to be widely known and implemented to be effective, and the OEWG should strengthen their successful and sustained application by States. Some States and regional organizations also face challenges and barriers in the implementation of the cyber CBMs recommended by the 2013 and 2015 GGEs. There may be a role for the OEWG in providing guidance in this regard also.

Because the OEWG has a broader scope than the GGE, and is open to a wider variety of actors outside of just States, Canada hopes that the OEWG report will address issues such as online freedoms and gender equality. Canada is pleased to note that the OEWG process will include multistakeholder meetings. We hope that the broadest possible range of civil society and private sector actors (NGOs, women’s groups, human rights organizations, academics, industry groups, tech companies, etc.), are included in this process and that their input is reflected meaningfully in an eventual OEWG report.

Canadian proposals for the 2020 OEWG report

In order to consolidate and build on the achievements of the last two consensus GGE reports, Canada proposes that the 2019-20 OEWG examine the following problem statement: what concrete actions could States take to ensure that a greater number of States can operationalize and implement the norms and CBMs endorsed in the two last consensus GGE reports? We believe that such a focus would allow the 2019-20 OEWG to make important progress by building on what was achieved in past GGE reports. This practical proposal builds on efforts that are underway in other forums, including the OSCE, ASEAN Regional Forum (ARF) and OAS. The 2019-21 GGE, which Canada will not be part of, may pursue some similar objectives. Close coordination between the work of the GEG and OEWG will ensure that their respective efforts are complementary and mutually supportive.

Canada would like the OEWG report to encourage countries to take actions, promote practices and cooperate in implementing the recommendations of previous GGE reports. For example, the report could urge countries that have not yet done so to implement cyber strategies that respect certain basic principles (including human rights); are aligned with the previously agreed norms and CBMs; and achieve certain broad outcomes. The 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 norms and CBMs in these forums over the coming years.
On cyber capacity building, the OEWG could offer concrete suggestions and call for greater mobilization of resources to assist States in implementing the recommendations of previous GGE reports. This would build on work being done on cyber capacity building in other settings (including the Global Forum on Cyber Expertise) and regional forums (such as the OAS).

Canada believes that as many diverse voices as possible should be included in the OEWG process and that the OEWG should take a transparent approach to all its work. This would include allowing and enabling civil society, women’s organizations, academics and private sector actors to engage with the OEWG and to make important contributions to an OEWG report. The contributions of civil society and non-governmental organisations are especially valuable in addressing issues such as online freedoms and gender equality issues, as well as in ensuring that States’ human rights obligations are taken into account in the drafting of the OEWG report. Specifically, Canada hopes that the OEWG can offer suggestions on how States can ensure that they respect their human rights obligations while developing and implementing their cyber security policies.

An OEWG report should also address gender issues, including the link between developments in the field of information and telecommunications in the context of international security and the Women, Peace and Security (WPS) agenda. We know that women are uniquely and differentially affected by conflict and threats to international peace and security. There is, however, little data on how this differentiated impact can be better understood and addressed within the field of ICTs in the context of international security. Canada therefore believes that the OEWG process should pay particular attention to placing gender equality and the meaningful participation of women at the centre of its efforts to prevent conflict and sustain international peace and security in cyberspace. It should explore how to increase the meaningful participation of women in international and national discussions, negotiations, strategies and capacity-building programs relating to the use of ICTs in the context of international security, taking place at the UN and elsewhere. For example, an eventual OEWG report could address how to better protect and prevent human right defenders (including women activists) from being targeted using ICTs.

These are only examples of possible topics, and it should be noted that the resulting proposals for State action would be voluntary and non-binding. We believe that these proposals would lay the groundwork for the development of a practical approach to implementing existing norms and CBMs. It would allow the OEWG to make important contributions on issues that are outside the GGE’s mandate, such as online freedoms and gender issues. It would also provide an opportunity to take stock of existing work done by the international community in these areas, to identify gaps and to explore avenues for future cooperation. We hope that the 2019-20 OEWG can reach a consensus report that incorporates some of the proposals outlined above in order to keep the momentum going and build on the achievements of the last two consensus GGE reports. Finally, the OEWG could consider producing outputs beyond just drafting a report. For example, the OEWG could decide to put together a compendium of best practices based on countries’ experiences in implementing their national cyber security strategies.