



Canada's submission to the United Nation Secretary General report on the scope, structure, and content of the proposed UN Programme of Action (PoA)

---

## Context

The digital domain has in recent years, shown negative trends that could potentially undermine international security and stability. These trends include the growing use of information and communications technologies (ICTs) for malicious purposes.

It is therefore imperative to address these potential threats, by establishing a permanent basis with which to build and maintain international peace, security, cooperation and trust in the ICT environment specifically through a cyber Programme of Action (PoA).

A PoA can be a key contributing factor as a permanent and inclusive venue within which UN member States can specifically address, and further elaborate on, shared commitments to promote peace, protect the acquis of responsible behaviour and avoid conflict in cyberspace. Canada's support of a PoA also entails further development in transforming societies and economies, and expanding opportunities for cooperation in the ICT environment.

In particular, Canada stresses that any new permanent mechanism is not intended to compete with what has come before it, or with what currently exists, but rather represents the next evolution in UN cyber discussions, building on discussions and agreements to date.

Canada recalls its support of the previous 2021 Group of Governmental Experts (GGE) consensus report, and in particular the 2019-2021 Open-ended Working Group (OEWG) report, which recommended that States consider proposals to advance practical work to implement our existing commitments.

Canada further recalls the substantive aspects of the OEWG's mandate, along with General Assembly resolution 73/27 which welcomed the effective work of the 2010, 2013 and 2015 Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security as relevant and guiding outcome documents to form the basis of the PoA.

## Objectives

The establishment of a UN cyber PoA to advance responsible State behaviour in the use of ICTs in the context of international security will support States' objectives in the following ways:

- allow for the continuation of previous consensus work in the GGEs and OEWG to consider, implement and advance responsible State behaviour in cyberspace and further build upon this work;
- Provide for genuine stakeholder participation;
- Create a single, dedicated, permanent forum to cyber, which will not require renewed iterations, under the auspices of the First Committee where States bear primary responsibility in matters of international security;
- Ensure an inclusive body in that it accommodates the interests of all UN States;
- Offer an action-oriented forum in that it addresses implementation of responsible State behaviour in cyber space, seeks to advance confidence building and promotes capacity building to enhance State's abilities to implement the norms of responsible behaviour and the implementation of international law;



- Address the needs of States to raise political awareness of cyber security issues domestically, anchored through a high-level conference and or political declaration; and
- Provide a forum for ongoing discussions around the future of the framework and its continued development in the face of emerging technologies and threats.

## Scope and Mandate

As a stable and permanent mechanism, the PoA would provide States with the flexibility to both maintain the existing framework, and develop it further as it evolves to address emerging and future threats.

On threats, the PoA could provide a platform to not only identify potential threats, but also to agree on solutions and put in place measures to mitigate against those risks.

The PoA could also build on existing work being done to operationalize the normative framework, i.e. the 11 agreed and UNGA endorsed GGE norms, by making use of the UNIDIR Survey of National Implementation and the Singapore-UNODA norms implementation checklist. For example, an early priority could be to encourage States to define, in a national capacity, what they consider to be critical infrastructure, which was an area of focus in the previous GGE consensus report.

Moreover, the full inclusion of relevant stakeholders in a PoA could help make progress on norm implementation and support States by promoting or assisting in regular self-reporting. The PoA could build on implementation surveys already in existence, in order to allow States to measure progress, as the implementation of norms will be a continuous process.

While norms are part of the international cybersecurity framework, greater understanding of how international law applies to cyberspace is equally important. With limited consensus or understanding *how* it applies, the PoA can encourage States to articulate their positions on international law. These can be collected, disseminated and discussed, in order to build further common understandings in this area.

The PoA could cement itself as a cooperative, multi-stakeholder model to help facilitate engagement with stakeholders, who in turn can assist in national and regional implementation efforts. The inclusion of relevant stakeholders in a dedicated forum would lend legitimacy and can shape an instrument that will reflect lived realities and address real threats.

A PoA could establish regional engagement through cooperation with regional organizations to facilitate coordinated initiatives. The United Nations Office for Disarmament Affairs (UNODA), through existing resources and voluntary contributions, should continue to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe, the Pacific Island Forum, and the Regional Forum of the Association of Southeast Asian Nations, to convene further series of consultations in order. These would allow member States of these organizations to share views on emerging threats, norms and best practices, application of international law, capacity building, confidence building measures, once the PoA is established in 2025 and onwards.



The PoA would provide a permanent mechanism to administer and evolve a directory of points of contacts at the policy and technical levels. This directory, which is currently being finalized at the OEWG, could also eventually expand to include, on a voluntary basis, the contact information of other stakeholders, in order to support more rapid crisis management when cyber incidents occur.

A PoA should leverage existing investments in capacity building and technical assistance as essential ingredients for implementation of the objectives listed above, as well as to facilitate cooperation between States. This would allow it to serve as an overarching confidence building measure in the field of information and communications technology security.

The PoA, based on needs identified by States themselves, would serve as a convening platform to match capacity building need and resources. Provisions of concrete support for capacity building will assist State's abilities to implement agreed norms, rules and principles. As a function, the PoA could also integrate existing tools for States and stakeholders to share relevant capacity building proposals such as the United Nations Institute for Disarmament Research (UNIDIR) Cybil Portal.

As an action-oriented mechanism, the PoA could cooperate with and leverage other capacity building efforts underway, through the Global Forum for Cyber Expertise (GFCE) or through UNIDIR. These collective efforts would help countries articulate and receive needed capacity building

## Structure

As set out in Canada's previous PoA [paper](#), important lessons can be learned from the set up of other PoAs, and from the number of recommendations on how to make the PoA a consultative and inclusive process. The establishment of a United Nations PoA should, in Canada's view, be structured and developed in the manner laid out below.

Once established, it is important to note that the PoA will not act as a treaty process, but as a political mechanism—intended to work by unanimous consent—for encouraging voluntary cooperation on promoting responsible State behaviour in cyberspace.

UNODA can serve as the Secretariat of the international conference and can act as the PoA's Secretariat. In addition to preparing the annual meetings and review conferences, UNODA would also be in charge of administering the global Point of Contact directory. Periodic reviews on the progress made in the implementation of the PoA, as well as the Programme's future work priorities, should be undertaken on a biannual basis. This should be done in order to keep pace with the speed of cyber developments.

As a permanent process, the PoA should not only focus on producing reports and outcomes. Instead, it must show sustained and measurable progress. A cyber PoA could fill the current accountability gap between the existing norms and actual practice by solidifying commitments and introducing or leveraging existing reporting or review mechanisms. It will be crucial to incentivise reporting practices by making use of the information they contain or offering opportunities to discuss them, such as in mandated meetings.

A minimum of two thematic meetings a year should take place in order to focus on areas to help drive collaboration and advance cyber issues.

Proposed working groups could include emerging threats, norms and best practices, application of international law, capacity building, confidence building measures.



Representatives in these working groups could meet at least once a year to track their progress on implementing the PoA and recalibrate efforts as needed. These meetings should be geared towards resulting in an outcome document containing conclusions that, if unanimously agreed, are politically (though not legally) binding for all participants in the PoA.

Decisions on substantive issues shall be adopted by consensus.

## **Proposed Next Steps**

The UNSG report, containing recommendations to the General Assembly, should be presented with a view to a decision being made by the Assembly at its seventy-eighth session, on the structure and content of the Programme of action and the preparatory work for its establishment.

No later than August 2024, an International Conference should be convened. It should include relevant international and regional organizations, as well as relevant non-governmental organizations, civil society organizations, academic institutions, the private sector and the technical community.

The purpose of the international conference would not duplicate the work of the OEWG. Rather, it would focus specifically on the modalities and substance of a PoA, including finalising and adopting a political declaration. This declaration would elaborate the key elements of a PoA, a programme of future work and a set of priorities for the work of the PoA, in accordance with the scope of the PoA, as mandated in UNGA Resolution 77/37. The PoA would not begin to meet until the end of the 2021-2025 OEWG and would take the OEWG's final report, should it be agreed by consensus, into account in its work. The sessions that take place in the PoA once it is established will also take into account the consensus reports A/65/201, A/68/98, A/70/174, A/76/135, and A/75/816, the 2023 annual progress report of the Open-ended working group established pursuant to resolution 75/240 and any future annual progress reports.

## **Modalities**

Given the nature of the cyber security field and the diffuse ownership of key cyber infrastructure and services, stakeholders will have an important role to play in implementing a cyber PoA.

In consultation with the UNODA, a list of representatives of other relevant non-governmental organizations, civil society organizations, academic institutions and the private sector, including those with expertise in the field of cybersecurity, will be drawn and presented to consider who may participate in the preparatory sessions, the international conference, and session of the PoA.

The PoA's stakeholder modalities should be based on Modalities for the Ad Hoc Committee on Cybercrime in order to enable the broadest possible level of participation from civil society, the private sector, and other relevant stakeholders.

The PoA should aim to be gender-sensitive and inclusive, and as a future instrument, find ways to reinforce human-centric approaches to international cyber peace and security.