Programme of action (PoA) to advance responsible State behaviour in the use of ICTs in the context of international security

Draft elements for Sweden's submission to the UNSG report mandated by UNGA Resolution 77/37

Introduction

The General Assembly First Committee has consolidated a framework for responsible State behaviour in the use of ICTs, endorsed by the General Assembly in consensus resolutions[1]. In the context of the framework, there have been discussions on the establishment of a "regular institutional dialogue" (RID) to address issues related to the use of ICTs in the context of international security. It has been underlined that such a RID should place a strong focus on supporting the implementation of the normative framework. In particular, the 2019-2021 OEWG concluded that any future RID should be *"an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based"*[2]. In this context, the establishment of a **Programme of Action** (PoA) would provide a a permanent institutional mechanism which would follow-up on the implementation of the agreed framework, while also allowing for its further development, if appropriate.

Content

The PoA could be based on a political document which would notably (i) reaffirm States' political commitment to the framework for responsible State behaviour, as affirmed in relevant reports and resolutions[3]. This founding commitment would consider the consensus outcomes adopted within the 2021-2025 OEWG; (ii) establish a permanent institutional mechanism to (iii) advance implementation of this framework, including by supporting States' capacities to do so, (iv) further develop the framework as appropriate, (v) foster multistakeholder cooperation in relevant areas.

Sweden notes that there are many aspects of how to advance the implementation of the framework. We align ourselves with the EU input and the French proposal as presented at OEWG in March 2023. As to further advance the discussion, our submission focusses on the importance of applying a multistakeholder approach, the role of the private ICT sector and the need to promote public private partnerships.

Multistakeholder involvement

Mindful that "States bear primary responsibility for the maintenance of international peace and security"[4], the PoA should seek to enhance multistakeholder engagement and cooperation for the benefit of an open, free, global, stable and secure cyberspace.

Today it may be difficult for governments to gather the means and capacity to fully understand and respond to the growing number of cyber related issues their countries are facing. Governments are increasingly relying on cooperation and collaboration with the private sector and other non-governmental actors to respond to the threats and challenges, and the public policy needs and concerns that stem from them. Meanwhile, the value of further strengthening collaboration, when

---

[1] See UNGA Resolutions A/RES/70/237, A/RES/76/19.

[2] Final report of the 2019-2021 OEWG, A/75/816, paragraph 74.

[3] This would include UNGA resolution A/RES/76/19, the 2010, 2013, 2015 and 2021 consensus reports of the groups of governmental experts, the 2021 report of the Open-ended Working Group, the first annual progress report of the open-ended working group 2021–2025, bearing in mind that the future consensus outcomes of the current 2021-2025 OEWG will add to this framework which is cumulative and evolving.

[4] Final report of the 2019-2021 OEWG, A/75/816, paragraph 10.

appropriate, with civil society, the private sector, academia and the technical community, was repeatedly emphasized by relevant First Committee working groups[5], both because cooperation with these stakeholders can be essential for States to implement their commitments under the framework, and because stakeholders themselves "have a responsibility to use ICTs in a manner that does not endanger peace and security"[6]. Private stakeholders can also bring valuable expertise to discussions and contribute to capacity-building efforts. Security in the digital era cannot be achieved by States alone and the multistakeholder approach must remain a fundamental part of our cooperation.

The role of private ICT sector in defending and promoting human rights
The ICT sector has often been perceived as an ally of freedom of expression and human rights. Telephones and cellular technology connect people and businesses; the Internet opens a new world of information, education and entertainment for people and businesses, enabling exchanges, debates, arguments, discussions, negotiations, and resolutions. The private sector provides the technologies that forms the backbone of the Internet.

The private ICT sector is very diverse. It comprises purveyors of hardware – such as transmission towers, instruments and equipment, servers, cables and other infrastructure – as well as software and digital services, including the numerous technologies and standards that comprise the architecture of the Internet . This diversity makes it difficult to generalise about the sector and focus on a single set of issues. As with other industries, companies from all around the world are active in the ICT sector, making a geography-focused strategy less effective and a multilateral approach necessary.
The obligation of States to respect human rights also includes an obligation to protect individuals and groups of individuals against human rights abuses by third parties, including business enterprises. Their obligation to fulfil human rights means that States must take positive action to facilitate the enjoyment of basic human rights (*UN Guiding Principles on Human Rights and Business, principle 1*). The possibility of a gap between users' and civil society's expectations and business's understanding of its responsibilities will always remain. There is a need for greater consensus politically and within the industry to work on this agenda.

Multistakeholder initiatives are the way forward
Governments and ICT companies need good guidance, based on internationally accepted standards, norms, and principles to respond to challenges. Sweden will continue to promote an open, free, global, stable and secure cyberspace where human rights, fundamental freedom and the rule of law fully apply in support of the social well-being, economic growth, prosperity and integrity of our free and democratic societies. Therefore, governments would benefit from working together and approaching problematic contexts jointly. The PoA mechanism should be a platform for States to engage with multi-stakeholders including the private sector from all regions of the world. Working in partnerships can add valuable input.

Sweden supports an approach that is anchored in norms, rules and procedures and practices. Yet, such regimes are difficult to put in place in constantly shifting environment. Overregulation may misalign with both existing and emerging security threats, and they can slow or undercut innovation and reduce the incentives and reduce the incentives for private sector participation. It can also misalign with other obligations and duties, including those aimed at minimizing harm to the public. The PoA mechanism must seek to engage with the private sector on cybersecurity and resilience related issues. In this regard, ensuring that public-private partnerships and multistakeholder engagement are underpinned

---

[5] Final report of the 2019-2021 OEWG, A/75/816, paragraph 22.
[6] Final report of the 2019-2021 OEWG, A/75/816, paragraph 10.

by key principles such as transparency and accountability, notably when they are established to solve specific public policy problems.

Keeping the momentum and prepare for an international conference in 2025
Sweden supports additional focused discussions in the 2021-2025 OEWG to further elaborate the PoA and seek consensus on its establishment. Intersessional meetings and dedicated sessions of the OEWG should be organized in 2024 and 2025 to continue elaborating the different aspects of the PoA, draft its founding document, etc.

Sweden supports further discussions on the precise modalities for the potential establishment of a PoA, including the option of a dedicated international conference in 2025, to adopt the founding document of the PoA, on the basis of the preparatory work done including in the 2021-2025 OEWG (as noted in UNGA Resolution 77/37). It should provide for participation by relevant stakeholders (accredited with modalities close to those adopted via resolution 75/282).