MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

TECH
ACCORD

Paris Call Working Group 3 – Supporting the Continuation of UN Negotiations with a Strong Multistakeholder Approach

Session 3 – The proposal for a Programme of Action and the way forward for multistakeholder dialogue on cyber

Wednesday, 8 September, 4:30-5:45 PM CEST

Context

Following the launch by the French Ministry for Europe and Foreign Affairs of six working groups aimed at advancing the principles of the Paris Call, the Cybersecurity Tech Accord has been tasked with leading the debate on multistakeholder inclusion in the UN negotiations on cyber (Working Group 3 or WG3). Since March, WG3 has held one kick-off meeting and two sessions where stakeholders looked at and debated i) examples of multistakeholder governance and ways these can be applied to the ICT security debate and ii) ways to ensure greater political cooperation amidst growing tensions in cyberspace. The sessions allowed us to gather great insights into how public, private sector and civil society stakeholders view multistakeholder governance, on the factors that have been holding back progress and, on the aspects to reflect on to advance the debate in this space.

Session 3 – Content and structure

This third session aims at presenting and debating the way forward for the Programme of Action (PoA), a proposal supported by over 50 states, to establish a permanent, inclusive, consensus-based and action-oriented international instrument to advance responsible behavior in the use of ICTs in the context of international security. In 2021, the PoA has been noted in the reports adopted by the UN Open-Ended Working Group (OEWG) and the sixth group of governmental experts (GGE) as a possible way forward to advance responsible state behaviour in cyberspace.

The PoA would not only reaffirm existing states' commitments to responsible behaviour in cyberspace but also work to support their capacities to effectively implement international cybersecurity norms. The PoA would as well promote constructive dialogue and engagement with other stakeholders, such as the private sector, academia and civil society.

Concretely, the PoA could encourage states to cooperate with other stakeholders, for example in areas such as the development of coordinated government and corporate policies to improve the security of the ICT supply chain and build trust; the responsible disclosure of vulnerabilities and prevention of the proliferation of malicious tools and techniques; support for research in relevant areas; the promotion of a culture of cybersecurity in the larger public.

The PoA could also encourage non-governmental stakeholders' participation in its works, for example by including exchanges with these stakeholders in the PoA meetings and/or giving them the opportunity to submit working papers to PoA meetings.

A draft food for through paper on the PoA is included in this note for easy reference.

The WG3 session will allow stakeholders to comment on this draft and to discuss the proposal's potential implementation.

MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

TECH
ACCORD

Draft Food for thought paper

Possible structure and content of a UN PoA on the responsible use of ICTs in the context of international security

53 States cosponsor the establishment of a UN Programme of action (PoA), as a permanent, inclusive, consensus-based and action-oriented international instrument to advance responsible behavior in the use of ICTs in the context of international security. While building on the acquis resulting from the work of previous UN Groups of governmental experts (GGE) and the Open ended working group (OEWG), the aim of the PoA would be to establish a standing institutional framework to make concrete progress in the implementation of the norms identified by these Groups. The PoA would therefore offer a platform to adopt operational recommendations, to promote international cooperation and foster assistance programs tailored to the needs of beneficiary States, notably in the area of capacity-building. The PoA would as well enable a regular institutional dialogue on issues pertaining to ICTs, including all States as well as other relevant stakeholders.

This paper is meant to provide elements for further discussions on the possible structure and elements of the PoA. Suggestions and remarks by all co-sponsors, interested States and other stakeholders are welcome.

The PoA could include (1) a political commitment to norms of responsible State behavior, (2) a set of recommendations for action at the national, regional and international level, (3) provisions to strengthen international cooperation between States and (4) to foster constructive engagement with other stakeholders, (5) a call for strengthened, better coordinated assistance, in particular in the area of capacity building, (6) an institutional mechanism to follow up on its implementation and discuss new challenges or priorities as appropriate.

1/ The PoA could include a preamble part, which would :

- recall existing and emerging threats to international security related to the malicious uses of ICTs, building notably on the threat assessments contained in GGE and OEWG reports;

- reaffirm the applicability of international law to the use of ICTs, as well as the commitment of States to the norms of responsible behavior (affirmednotably by the 2015 GGE report and the 2021 OEWG report);

- decide to establish a PoA, to advance the effective implementation of these norms, facilitate sustained international cooperation and assistance, and, as appropriate, and develop additional norms and rules as appropriate.

2/ The PoA could then make recommendations for actions and policies at the national, regional and international level, to improve the effective implementation of the norms of responsible behavior:

- at the national level, States could be encouraged, inter alia,
    - to adopt and apply relevant legislation and policies to investigate and address the malicious use of ICTs on their territory;
    - to identify critical infrastructure located on their territory, and take adequate measures to ensure their protection;
    - to establish CERTs/CSIRTs with a clear mandate, and refrain from using them to carry out malicious activities;

- to designate diplomatic and technical experts as points of contact for international exchanges and incident management;

- States could also be encouraged to conduct a gap analysis of their needs in terms of capacity (for example, the PoA could mandate UNIDIR to develop a voluntary self-assessment tool to help States conduct such an analysis).

- Regional organizations could be encouraged,
  - to develop instruments and policies to tackle the malicious use of ICTs;
  - to put in place mechanisms for information exchange between Member States;
  - to develop cooperative mechanisms to handle incidents: States could be encouraged to request for assistance if needed when their critical infrastructure is subject to malicious activity, and voluntary templates could be developed for such requests.
  - to foster cross-border cooperation (in particular to protect critical infrastructures that provide services to several States);
  - to initiate assistance and capacity-building programmes that take into account the specific needs of States in the region, etc;
  - to develop and implement confidence building measures.
- The PoA could include an annex which would list relevant initiatives taken by regional organizations.

- At the international level, in addition to the same functions of the PoA at the regional level, the PoA could also encourage consultations to facilitate the peaceful settlement of disputes, the compilation of national good practices in UN databases. The PoA could also encourage cooperation to address the criminal and terrorist use of ICTs in accordance with its mandate, etc.

3/ The PoA could offer a framework to develop international cooperation between States. To that end, the PoA could :

- encourage confidence-building and transparency measures: States could be encouraged to share, on a regular basis, national reports on their efforts to implement the PoA. They could also be encouraged to share best practices, national contributions regarding their approaches to the designation of critical infrastructure, the attribution of ICT incidents and the management of such incidents, their understanding of how international law applies to the use of ICTs, etc.

- These national reports and contributions could be discussed during annual meetings of the PoA and made available on a common portal.

4/ While being a State-driven process, the PoA could also promote constructive dialogue and engagement with other stakeholders, such as the private sector, academia and civil society.

- It could encourage States to cooperate with these stakeholders in particular to :
  - develop coordinated government and corporate policies to improve the security of the ICT supply chain, and build trust;
  - organize the responsible disclosure of vulnerabilities and prevent the proliferation of malicious tools and techniques;
  - encourage research in relevant areas;
  - promote a culture of cybersecurity in the larger public.

- Future annual meetings of the PoA would include an agenda item dedicated to exchanges with the private sector, academia and the civil society.
- These other stakeholders could be encouraged to submit working papers to PoA meetings.

- While the PoA would remain a State-driven process, it could allow for informal discussions with other stakeholders to consider relevant issues..

5/ The PoA could also foster international assistance, with an emphasis on capacity building to develop national ownership and enable States to implement the norms of responsible behavior.

- The PoA would encourage States and organizations in a position to do so to engage in assistance and capacity building projects, taking into account the needs identified by States in their national self-assessment and gap analysis.

- Annual meetings would provide an opportunity to discuss ongoing efforts at the national, regional and international levels, and discuss avenues for better coordination between different donors and different initiatives. States could also consider the possibility to establish a funding facility, such as a trust fund, to support cooperation and capacity-building projects.

6/ The PoA would establish a regular institutional mechanism to follow up on its implementation and address new topics as appropriate.

- The PoA would provide a lasting institutional framework for sustained dialogue and cooperation. Follow-up meetings could take place every [year], and review conferences every [four] years, to update the PoA and discuss additional norms or instruments as appropriate.

- This instrument would remain flexible : follow-up meetings could create new agenda items to address potential new challenges and priorities as they arise.

- The PoA can Function under the rules of procedure relating to the committees of the General Assembly with such modifications as the Commission may deem necessary and shall make every effort to ensure that, in so far as possible, decisions on substantive issues be adopted by consensus./.