Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

Directorate of Political Affairs DP
Division for Security Policy DSP
Office of the Sepcial Envoy for Cyber Foreign and Security Policy

Position Paper on Switzerland's participation in the 2019-2020 UN Open-ended Working Group on «Developments in the Field of Information and Telecommunications in the Context of International Security» and the 2019-2021 UN Group of Governmental Experts on «Advancing responsible State behavior in cyberspace in the context of international security» - January 2020

Purpose

This paper outlines the positions of Switzerland on the two UN-processes related to cybersecurity and the topics discussed within them.

Summary

Switzerland supports and is committed to both UN processes on cyber in the context of international security. The two processes should, in line with their individual mandates, work in parallel to prevent duplication and ensure coherence and mutually reinforcing outcomes. Switzerland will encourage members of the Open-ended Working Group (OEWG) and UN Group of Governmental Experts (UN GGE) to consolidate and build on the progress made in the 2010, 2013 and 2015 UN GGE reports. Switzerland supports the consensus reached in these reports that international law applies to the activities of States in cyberspace. Switzerland believes that the universality of the OEWG provides an opportunity to create wider understanding of the topic and make progress in implementation, operationalisation, and universalisation of already agreed upon recommendations. Switzerland also believes that the continued expert discussions in the framework of the UN GGE can efficiently provide valuable expert input to discussions at UN level and elaborate concrete guidance on how to operationalise agreed recommendations. Switzerland cautions against reopening norms, rules, and principles that have already been agreed upon.

---

1. General Position

- Switzerland welcomes the increased attention paid to cyber issues at the UN.
- The cyber domain reaches every facet of our lives and permeates almost every aspect of our societies. It offers a myriad of new opportunities for our societies and economies, and can be a driver for positive change and stronger cooperation.
- Malicious activities in cyberspace affect every country and can have serious negative consequences for international peace and security, the protection of human rights, and the international community's efforts to implement the 2030 Agenda.
- An open, free and secure cyberspace is key to ensuring that we can all take full advantage of the huge potential that the digital age offers.
- Thus, preserving the openness and freedom of cyberspace while protecting it against looming security threats is one of the main challenges.
- States have a common interest and a shared responsibility to ensure that cyberspace is used in a peaceful way, and that it continues to serve as a multiplier – both for social and economic development and for the enjoyment of human rights and fundamental freedoms.

- Switzerland welcomes and supports the consensus reached by the UN GGE reports of 2013 and 2015 that international law applies to the activities of States in cyberspace. Switzerland welcomes the international norms and principles contained in the UN GGE report of 2015. Switzerland believes that it is now time to move forward and support operationalisation of international law in the ICT environment.
- Switzerland cautions against reopening norms, rules, and principles that have already been agreed upon. This would put at risk the progressive successes of past UN GGEs.
- Switzerland is convinced that the UN needs to continue to play a leading role in furthering the international community's understanding of existing and potential cyber threats as well as of cooperative measures designed to address them. To this end, it is crucial to build on the progress achieved so far in order to help consolidate, universalise and operationalise the 2010, 2013 and 2015 UN GGE recommendations endorsed by the GA.
- Switzerland is pleased that the OEWG format allows the wider UN membership to deal with international cyber security needs as well as allow for a broader and more inclusive participation, involving interested non-state actors, such as business, non-governmental organisations, and academia. We will encourage the UN GGE to consider input of such actors.
- As a member of the OEWG and GGE, Switzerland will continue to advocate for the promotion of international cyber stability that is based on the application of international law, voluntary norms, rules and principles of responsible state behavior, confidence building measures, and capacity building.

2. How the two groups can work best together

- Switzerland participates in both UN processes and is fully committed to both of them.
- Switzerland welcomes the multi-stakeholder approach of the OEWG and believes that this is key for the success of the OEWG. It offers a unique opportunity to build wider understanding of the topic.
- Switzerland's view is that the two processes should work in parallel to ensure coherence. The two processes should be mutually reinforcing and there should be a functioning information exchange between them.
- Both processes should build on progress made over the last years and should not fall behind what has already been achieved by the past UN GGEs.
- A key task is to avoid contradiction, fragmentation or duplication in the activities of the two processes. Until now, the UN membership has progressed in a unified and cohesive manner on cybersecurity issues and it is crucial that this is maintained.
- Both processes have very similar mandates and will to a large amount address the same topics. With a view to increasing efficiency, it could therefore be useful to clarify, which process could yield results faster in certain areas. These results would then be fed into the other process.

3. General positions on agenda items

3.1 Existing and potential threats

- Switzerland increasingly observes a stronger diversification, specialization and professionalization with regard to cyber operations. Operations conducted through the cyber domain have become more targeted, complex and sophisticated; their execution requires high skills and expertise. This, in turn, increases the risk of miscalculation and misunderstanding between states.
- Switzerland is concerned by the fact that cyberspace is increasingly becoming a sphere of power projection. Thus, States are using cyberspace to advance national security

interests. Acts transcending national boundaries and challenges linked to attribution of cyber operations are characteristics of cyberspace.

- While the majority of cyber operations have so far been executed in a precise and targeted manner from a technical point of view, we have recently seen cases within which cyber tools were used at random and causing unintended harmful effects. In addition, we observed a lowered threshold to conduct malicious cyber activities with harmful effects.
- Such cyber operations can have indirect and unintended harmful effects and generate damage to vital services/critical infrastructures and systems.
- Healthcare is among the most vulnerable systems and has recently come to be exposed to cyber threats.
- Cyber has also become an additional vector to spread disinformation and influence public opinion in order to undermine trust and confidence in political and democratic processes and institutions.
- Lastly, due to the continuous digitalization of processes and the roll-out of new technologies to support this development, the supply chain grows increasingly complex and interdependent. Interference or limitation will have ever-growing disruptive effects in terms of security and reliability.
- In general, the OEWG and the UN GGE should focus on those cyber threats that could have serious implications for international peace and security.

3.2 International Law

- The promotion of a strong international legal order governing activities in cyberspace is in Switzerland's view essential for the prevention of conflict, to sustain peace in cyberspace, as well as for stability and accountability.
- The digital domain is a multiplier for democracy and human rights: it gives people a voice, a chance to express themselves freely, and gives them unprecedented access to information. Switzerland believes that people should enjoy the same rights online that they enjoy offline.
- Switzerland welcomes the efforts undertaken by the 2010, 2013 and 2015 UN GGEs to enhance the understanding of the application of international law to cyberspace. The 2013 and 2015 consensus reports stated and confirmed that international law applies to the activities of states in cyberspace.
- Switzerland is of the view that international law, including the UN Charter and international humanitarian law, apply and govern activities in cyberspace.
- The non-exhaustive reference to a number of international law principles in the UN GGE 2013 and 2015 reports is a strong affirmation of the rule of international law in cyber space. Switzerland would like to recall in particular the principle of State sovereignty, sovereign equality, the settlement of disputes by peaceful means, the prohibition of the use of force, non-intervention in the internal affairs of other States, and the respect for human rights and fundamental freedoms.
- The specific characteristics of cyberspace, such as the absence of territorial borders, the enormous speed of operations, and the challenges linked to attribution, raise a number of questions to be discussed further, as to how international law applies in practice.

3.3 Rules, norms and principles for responsible State behavior

- The UN GGE consensus report of 2015 provides a substantial list of recommendations as to how states should behave in a responsible way. In Switzerland's view, this is a milestone as it contributes to setting the standard for responsible state conduct.
- Norms, rules, and principles for the responsible behavior of States have an important stabilizing potential. Switzerland believes that efforts should be concentrated on the

consolidation of the consensus reached by previous UN GGEs. In Switzerland's view, it is time to focus on operationalising existing rules and to share positive national examples of implementation.

- While doing so, a clear distinction should be made between binding international law principles and voluntary, non-binding norms.

3.4 Confidence-building measures

- Building confidence between states is vital. Confidence-building measures (CBMs) strengthen international peace and security and can increase interstate cooperation, transparency, predictability and stability.
- The 2015 UN GGE report contains very useful proposals for CBMs designed to increase interstate cooperation, transparency, predictability, and stability. Implementing these measures is a low-hanging fruit that will enhance transparency and build trust.
- Switzerland is committed to the globalization of the work conducted at the regional level and will continue to support universalisation of CBMs developed at regional level under the auspices of the OSCE.

3.5 Capacity-building

- In order to contribute to an open, secure, stable, accessible and peaceful ICT environment, all states need to be able to address cyber security risks at the technical-operative level and to participate in a meaningful and constructive way in policy level fora.
- Capacity building is key to broaden state cooperation in the areas of CBMs and norms, rules and principles of responsible state behavior.
- Switzerland believes that bilateral and multilateral cooperation initiatives can help improve the environment for effective mutual assistance between states in their response to ICT incidents.
- The specific needs of developing countries should be taken into consideration when states identify measures to support capacity building.
- Capacity building efforts contribute to bridging existing digital divides. Switzerland will continue to support these efforts.