



Amb. Jürg Lauber

Chair of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020

Bern, 9 April 2020

UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020
Written feedback by Switzerland to the first pre-draft report of the OEWG

Dear Mr. Chair, dear Jürg,

Thank you very much for consulting us on the pre-draft report of the OEWG. We would like to express our appreciation to you, your team and the Secretariat for the continued efforts to a successful completion of the work of the OEWG. We acknowledge that it is a challenging task to try to reflect the various points of view brought forward in the OEWG and would like to congratulate you and your team for your remarkable efforts to comprehensively reflect the discussions. We would like to express our support for the pre-draft as a basis for the report of the OEWG. Please find below our feedback, thoughts and considerations, which we hope will be helpful to you for the preparation of the report.

I. General remarks

Switzerland is particularly committed to building and ensuring an open, free, secure, stable, accessible and peaceful cyberspace, which furthers protection and enjoyment of human rights, enables economic development and contributes to sustaining peace. It is in our common interest to ensure that cyberspace is governed by the rule of law and used in a peaceful way. Ensuring that existing rules of international law are applied and respected in cyberspace is a key priority for Switzerland. We welcome the progress and work achieved by the UNGGEs reflected in the three consensus reports of 2010, 2013 and 2015. They confirm that international law applies to the activities of States in cyberspace. It is crucial for the report of the OEWG to highlight that the GGE reports reflect consensus between States and are the starting point and basis for discussion (“acquis”), as they establish the framework for responsible behavior of States in cyberspace based on international law, voluntary norms, confidence-building measures and capacity building. States agreed that the work of the OEWG should be based on this consensus and that there should be no “rolling back”, but rather progress in operationalising the framework.

When referring to the outcomes of the past GGE reports, it is important to carefully reflect agreed language throughout the report, such as for example that the UN Charter is applicable “in its entirety”.

In our view, the pre-draft overall gives an objective and accurate picture of the discussions at the OEWG. At the same time, due to the wording chosen at the beginning of several paragraphs or the lack of consistent use of qualifier language respectively, we believe that the nuanced discussions led at the OEWG are not always fully reflected and not all aspects or viewpoints brought forward by delegations are presented equally. We suggest that the language chosen in the report be streamlined bearing this in mind.

We welcome the importance the report gives to the need to narrow the “gender digital divide” and of promoting effective and meaningful participation and leadership of women in multilateral processes such as the OEWG. We believe that the gender dimension of cyber security, including the need for more gender-related data to address the gender impacts of cyber security policies and capacity building efforts, should be mainstreamed throughout the report.

We welcome reference to a multi-stakeholder approach in the report and the usefulness of the intersessional informal consultations. These references highlight the importance of a multi-stakeholder approach to the ICT environment. Switzerland would like to suggest integrating this understanding throughout the report, including by highlighting that non-state actors have an essential role to play in contributing to building trust and confidence in the use of ICTs, as well as in supporting implementation of the framework of responsible behavior of States in cyberspace. Also, involvement and meaningful participation of non-state actors should be maintained and formalized for future institutional dialogue and this should be reflected in the report.

The proposed conclusions and recommendations also reflect, in our view, the discussions in our group and provide a good basis for further deliberation. The majority of the proposed recommendations address various concerns expressed over the course of our work to date. At the same time, we identified room for further clarification and sharpening of the conclusions and recommendations.

II. Detailed remarks

A. Introduction

Paras. 1, 3, 8

Switzerland agrees that the report of the OEWG be situated in the broader perspective and purpose of the United Nations. It has long been acknowledged that the three pillars of the UN – human rights, sustainable development and peace and security – are interdependent and mutually reinforcing. We believe that this “cross-pillar” approach to the prevention of conflict and the maintenance of international peace and security could be brought out more strongly.

Para. 3

Switzerland agrees with expanding on the dual-use nature of ICTs in the introductory section of the report. At the same time and in line with the discussions at the OEWG, this paragraph could focus more clearly on the existing agreement that States engage for a peaceful cyberspace and peaceful use of ICTs.

Para. 12

Switzerland welcomes the remarks made in this paragraph.

B. Existing and Potential Threats

In line with the guiding question for the second OEWG session relating to the assessment of existing and emerging threats as outlined in the GGE reports of 2010, 2013 and 2015, Switzerland believes that it would be important to reflect that this assessment remains valid. Also, we agree with the assessment that increasing connectivity and reliance on ICTs may bring unintended risks, as well as unintended consequences and unintended harmful effects.

Para. 14

We believe it is important to specify that not only the possession by non-state actors of ICT capabilities previously limited to States is of concern, but also the possibility that these ICT capabilities could be used for malicious purposes by these actors.

Para. 15

While we agree in principle with the content of this paragraph, in our view, it should be adapted to better reflect the nuanced discussion held at the OEWG. Indeed, we do not believe the report should reflect this discussion as having focused on the “militarization” of cyberspace. Rather, it was noted that the development or use of offensive ICT capabilities, as well as the stockpiling of vulnerabilities can have a destabilizing effect on international peace and security if ICT capabilities are used in a manner inconsistent with a State's obligations under international law. In addition, we would like to highlight that whenever a State decides to apply an active measure, the State must abide by existing rules and adhere to international law, including the UN Charter in its entirety. These aspects should be reflected in the report.

We agree that ICTs should not be used to interfere with internal affairs of a State and suggest that the report emphasize the concerns that cyberspace can be misused to undermine trust and confidence in the political and democratic processes of a State.

Para. 17

Switzerland supports the analysis and aspects expressed in this paragraph. Threats stemming from the malicious use of ICTs by States can affect different groups of people differently. Also, different groups can be vulnerable to different cyber threats and in different ways than others. As stated in the pre-draft, groups vulnerable to cyber threats can for example include youth, the elderly, women and men. Switzerland holds that it would be useful for the report to reflect agreed language on vulnerability aspects, as included in existing agreed international texts.

Para. 18

Switzerland welcomes this paragraph.

Para. 19

Switzerland, including with a view to the current global crisis, believes that the report should also reflect the human cost of attacks to critical infrastructure, in particular the health sector.

We agree that global systems upon which public or financial systems rely can constitute transborder or transnational critical infrastructure.

C. International law

Switzerland holds that it is crucial for the OEWG report to highlight that, as stated by the GGE reports, international law applies to the use of ICTs by States.

Switzerland agrees that the rule of law in cyberspace is key for stability and predictability in relations between States. It is important to acknowledge and reflect in the report that adherence to international law, including international humanitarian law and international human rights law, is fundamental for security, stability, trust and predictability in cyberspace.

Also, as many other delegations at the second session of the OEWG, Switzerland drew attention to the Joint Statement of the Freedom Online Coalition on “Human Rights Impact of Cybersecurity Laws, Practices and Policies”. The statement recognizes that cybersecurity and human rights are complementary, mutually reinforcing, and interdependent. It highlights – in line with the recognition of the OEWG that cybersecurity is to be considered through a human-centric lens – that a human rights based approach to cybersecurity is a basis for strengthening cybersecurity and promotion of stability in cyberspace. A number of international human rights are of particular importance, namely the right to privacy and freedom of expression and information, as well as non-discrimination. In our view, this should be reflected in the report.

Para. 24

The paragraph reflects that States exchanged views on the relevance and applicability of specific bodies of international law (such as international humanitarian law, human rights law, international criminal law). This paragraph should also reflect that States not only discussed applicability but also application of these bodies of international law, in particular international humanitarian law and human rights law. As customary international law is a source of international law and not a specific body of law, it should not be mentioned in this listing.

This paragraph would also provide a good space to include reference to statements made by many delegations reaffirming that international humanitarian law is applicable to cyberspace in situations of armed conflict.

Para. 25

We welcome the important statements on international humanitarian law in this paragraph. It recalls the object and purpose of international humanitarian law and correctly stresses that international humanitarian law should not be misunderstood as legitimising the use of force between States, which is governed by the UN Charter. We further believe that this paragraph should also reflect discussions relating to the protection of critical infrastructure/civilian objects in situations of armed conflict.

Para. 27

In our view, this paragraph contains different and distinct points that could usefully be integrated into other existing paragraphs in order to better differentiate the topics. We therefore suggest separating the two main questions raised:

- Further clarification of questions relating to existing international law;
- The need expressed by some delegations for a new legal instrument/identification of need for new rules and codification.

With regard to international humanitarian law we would like to suggest to refer to the principles of “humanity, necessity, proportionality, distinction and precaution” instead of “including the protection of civilians and civilian objects”. This would build on the 2015 GGE report while also mentioning the equally important principle of “precaution”.

We agree that questions relating to how international humanitarian law applies to cyberspace were raised. However, the wording currently chosen (“prudence”) does in our view not accurately reflect existing agreement on the obligation of States to protect civilians and civilian objects also with respect to ICT incidents. We therefore suggest deleting the reference to prudence regarding international humanitarian law in this paragraph.

Para. 29

This paragraph in our view also reflects two distinct points that should be separated:

- It is important to note that it is not unusual for existing international law to be interpreted taking into account new developments. This is not exceptional or exclusive to developments in the field of ICTs. Therefore, we would like to see this reflected in the report, while refraining from using the term “progressive development”, as this does not accurately reflect the topic in question
- The need expressed by some delegations for binding measures is already covered in previous paragraphs.

Para. 32

Switzerland welcomes the references to peaceful settlement of disputes and the refraining from threat or use of force in this paragraph.

This paragraph combines two topics that are distinct and should be reflected accordingly:

- Importance of adherence to UN Charter principles and the UN Charter in its entirety. This paragraph reflects the key recognition that a peaceful cyberspace is a common goal of all States. Therefore, this important paragraph could be moved up.
- Attribution: In line with our statements and the intervention of others at the OEWG, it is our view that attribution is a national prerogative. We are convinced that the report would provide a significant added value by referring to attribution as a process which takes into account the technical characteristics of an attack, the wider context, the full range of information gathering and the legal criteria as set out in the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts. This process lays the basis for political decision-makers to attribute an attack to a specific actor. We would therefore welcome the explicit reference to “national prerogative” in this paragraph. Given the multifaceted nature of attribution, it would make sense to mention the process of attribution under "D: Rules, Norms and Principles for Responsible State Behaviour".

D. Rules, Norms and Principles for Responsible State Behaviour

Switzerland agrees that voluntary norms do not replace or - equally important - alter international legal obligations. In our view, this is a key aspect that should be reflected clearly throughout the report.

Para. 34

We believe the report should exercise prudence when describing discussions on topics outside the OEWGs mandate.

Para. 36

In our view, while the documents mentioned in this paragraph were indeed mentioned by some States over the course of the two OEWG sessions, they were not discussed or elaborated. We would therefore suggest removing this paragraph.

Paras. 37, 38

As we have expressed over the course of the work of the OEWG, Switzerland is of the view that voluntary norms reinforce international law and play an important role in preventing conflict. At the same time, it is clear that the mere existence of voluntary norms alone does not suffice to reach this goal; rather, respect and implementation of the existing voluntary norms is key to preventing conflict. In our view, the OEWG should focus on providing guidance on how existing norms can be operationalised. For example, proposals relating to the protection of the public core of the internet, not to harm medical facilities, not to disrupt infrastructure essential to political processes and relating to transnational critical infrastructure could in our view provide valuable guidance to existing norms.

Also, Switzerland would be grateful for clarification on what is meant by “upgrading” of voluntary norms. States have accepted to be guided by the 11 voluntary norms, as endorsed by the General Assembly. Therefore, Switzerland supports proposals aimed at encouraging the international community to reaffirm its commitment to international peace and security in the use of ICTs.

E. Confidence-building Measures (CBMs)

Para. 43

Switzerland supports the assessment that the OEWG in itself is a CBM. The OEWG provides an important space to strengthen collective implementation of the existing framework that guides the responsible use of ICTs by States, as developed by past GGEs and endorsed by the GA. We suggest that this paragraph is reformulated accordingly.

Para. 44

Switzerland welcomes the reflection of proposals made regarding establishment of national Points of Contact as well as a global directory. When referring to possible categories or levels of such Points of Contact, we would encourage consistent enumeration of such categories throughout the report (see also para. 68).

F. Capacity-building

We recommend that the section on capacity building refer clearly to different aspects and elements of capacity building, including the need for capacity building efforts to address gaps in both technical and policy capacity among all stakeholders, and to involve all stakeholders in addressing those gaps. Also, the report, including its recommendations, should highlight the need to make use of existing platforms or mechanisms aimed at coordination and coherence in capacity-building efforts and to avoid duplication of such existing efforts.

Para. 50

Switzerland agrees with the reflection in para. 33, whereas a need for additional efforts to build capacity in the area of international law was identified; this aspect should also be reflected here.

Para. 52

As we had mentioned during discussions at the OEWG, Switzerland strongly supports integration of agreed principles for capacity building in the report. We support the principles mentioned in this paragraph that in our view are all of equal importance.

G. Regular Institutional Dialogue

Switzerland supports the general gist of this chapter that reflects the recognition by States of the need for continued conversation at UN level about cybersecurity and responsible behavior of States. In addition, discussions at the OEWG made clear that there is a need to have a clear and shared understanding of what questions the international community should discuss at UN level, in order to decide on the format in which these questions could be discussed. As many delegations have said, “form follows function”. This aspect should be reflected in the report.

H. Conclusions and Recommendations

In our view, the report should provide targeted recommendations that can have real positive impact. We believe that the proposed recommendations could be prioritized with this goal in mind.

Para. 67

As stated in our feedback relating to chapter “D”, we hold that it is key for the report to reflect that voluntary, non-binding norms do not alter existing international law. Also, it is important to note that – as opposed to voluntary non-binding norms - international law goes beyond defining expectations of State behavior, but requires adherence. Being clear on this distinction in the report will significantly contribute to the better understanding of the relationship between voluntary norms and international law. In addition and as stated above relating to paragraph 43, we believe that dialogue on matters pertaining to cybersecurity will contribute to strengthening collective implementation and operationalisation of the existing framework for responsible behavior in cyberspace.

Para. 68

We welcome the focus on inviting and encouraging States to continue to share national views and practice on how international law applies to State use of ICTs. For Switzerland, this is a

key element of the report. Based on the consensus that international law applies in cyberspace, it is now up to States to elaborate on how they apply existing international law in cyberspace. And indeed, we agree that the result of these reflections should be shared with the international community in order to work towards a common understanding. At a later stage, other measures aimed at clarifying how international law applies in cyberspace, possibly also reflecting on convergence and divergence among state views, could be envisaged (such as for example a study by the International Law Commission). Currently, however, we should focus on and encourage States to elaborate and share their national positions on how international law applies in cyberspace.

Relating to recommendations on CBMs, Switzerland would like to propose to add a recommendation that would encourage States to consider cooperative activities that might contribute to confidence building in the field of ICT such as workshops, trainings and exercises, including tabletop exercises, with participation of governments, the private sector, and academia.

We hope that these reflections will be useful to you and your team. Please do not hesitate to contact us should there be a need for clarification or further questions.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'N. Olivieri', is positioned above a thin vertical line that extends downwards.

Nadine Olivieri Lozano
Ambassador, Head of Division