IGF 2017 Reporting Template

- Session Title: Future scenarios for global cooperation in cybersecurity

- Date: 20 December 2017

- Time: 17.20 - 18.20

- Session Organizer: Qendresa Hoxha, Federal Department of Foreign Affairs of Switzerland

- Chair/Moderator: Jovan Kurbalija, Geneva Internet Platform

- Rapporteur/Notetaker: Barbara Rosen Jacobson, Geneva Internet Platform

- List of Speakers and their institutional affiliations:

- Frank Grütter, Ambassador, Head of the Division for Security Policy, Federal Department of Foreign Affairs, Switzerland, UNGGE 2016-2017 Expert
- Adrian Perrig, Director Network Security Program, ETH Zurich
- Alexander Klimburg, Program Director, Global Commission on the Stability of Cyberspace
- Katherine W. Getao, ICT Secretary, Ministry of Information Communication and Technology of Kenya, UNGGE 2016-2017 Expert
- Elina Noor, Director Foreign Policy and Security Studies, Institute of Strategic and International Studies (ISIS) Malaysia
- Belisario Contreras, Cybersecurity Program Manager, Organization of American States

- Key Issues raised (1 sentence per issue):

The inability of the UNGGE 2016/2017 to reach consensus on a further report has raised many questions. What does this development mean for international cybersecurity? Is it time to think of new formats for global cooperation in cybersecurity? Where should discussions on norms, rules and principles for responsible behavior in cyberspace be held? Where should the priorities lie?

- If there were presentations during the session, please provide a 1-paragraph summary for each presentation:

A. Perrig presented the ETH-project "SCION". It is a clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. Thus, it can render technically impossible many types of cyber-attacks.
A. Klimburg elaborated on the work of the Global Commission on the Stability of Cyberspace which was established in the beginning of 2017. Governments, private companies and academia are involved in its work. The Commission has released a recommendation for a norm on the protection of the public core of the internet and will be elaborating further recommendations (also based on work that is being conducted in other fora) to strengthen the stability of cyberspace. The international community can then discuss the exact meaning and possible implementation of the norms suggested by the GCSC.
K. Getao spoke about the consequences of the failure to reach consensus on a UNGGE report 2016-2017 and the missing of an institutionalized structure for the cybersecurity discussion for the global cyber-community in general and developing countries specifically. She mentioned that the "balkanization" of the cybersecurity debate might be a considerable risk. Developing countries would lose the opportunity to participate in the debate and understand cyber-related issues. There would be a lack of coordination among countries which would then lead to different priorities in the fight against cyber risks.
E. Noor provided a legal as well as a regional perspective (Southeast Asia). She mentioned that the UNGGE report 2015 offered an excellent basis and already a lot of clarity on the applicability of international law in

cyberspace. The UNGGE Reports are documents that have been elaborated in consensus. Nevertheless, there is space for interpretations and therefore need for more clarity concerning the applicability of certain provisions particularly in the recourse to measures by states affected by cyberattacks.
She stressed that especially in Southeast Asia there will be greater prominence on the issue of content or information security. The question is how international law may play a part on the issue of content.
B. Contreras highlighted the need for capacity development and an inclusive approach to cybersecurity. The OAS has established a working group on cooperation and confidence building measures (first meeting will be in February 2018). He mentioned that the inter-american process is very inclusive as all members are able to participate, including civil society and private sector. He underlined the need for capacity building in the region. More awareness rising for the issue and more readiness to face cybersecurity threats is needed. Therefore, the OAS is promoting national strategies, providing training for law enforcement and information sharing.
F. Grütter mentioned different options for the involvement of the United Nations in the debate on cybersecurity. The continuation of the UNGGE process is one of different options, although generally speaking, there is no appetite for more of the same. For a 6th UNGGE there should be an increased number of members, a mechanism making informal consultations prior to the UN GGE meetings possible, and involve technical experts and civil society. Other options were also mentioned: a UN Open-ended Working Group on ICT security or a Committee on the Peaceful Uses of ICT (COPUICT) for instance.

- Please describe the Discussions that took place during the workshop session (3 paragraphs):

The possible technical solutions were discussed, especially the question whether they would be able to solve problems on the political/strategic level. It was said that the infrastructure has many vulnerabilities and that there was not one only solution to tackle all these vulnerabilities. In addition, there is a need to switch perspective from technical considerations and include human considerations into the analysis. Often, people are the weakest link so it is crucial to think of how do we address the human situation?
There was also a discussion on the remaining inequalities and the lack of capacities in cybersecurity specifically related to the UN GGE. The UNGGE 2016-2017 had 25 participating countries. Overall (over the total of 5 UNGGEs) 35 countries have participated in the group. This is considered being too exclusive and more capacities of developing countries are needed to level the playing field.
The lack of coordination was also discussed as well as the lack of a voluntarily accepted base line. There are many agreements but there are still many countries that are not aligned. Therefore, a common focus and more coordination is needed when it comes to international cybersecurity.

- Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways (3 paragraphs):

The panel came to the conclusion that capacity building is essential, especially in developing countries. On the one hand the systems in these countries need to be secured and on the other hand states need to obtain the know-how about the political cyber-agenda in order to be able to participate in and contribute to the international cyber-related fora.
The human factor should be included in the analysis of technical cybersecurity solutions. To this goal, the ETH in Zurich has started looking at protocol verifications and creating automated systems to verify the whole system, including the humans. The system should remain secure, even if the people make mistakes (lost password etc.).
The problem of the equal playing field was said to be a general problem not only present in the cybersecurity discussion. The solution of this problem is also linked to capacity building and to more inclusion. Excluding a part of the population means not being secure in cyberspace.
Regarding future formats it was said that it is important to first look into existing mechanisms (also within the UN) which are dealing with cybersecurity issues. On that basis gaps can be identified and it can be decided, whether or not new mechanisms and new fora are necessary. For any new forum inclusivity and transparency were said to be key characteristics. It needs to be a forum that allows bringing the discussion forward substantially but also renders the implementation of agreed measures possible.

From the legal perspective it was agreed that the application of international law should be affirmed and promoted. Experts should raise awareness of the existing legal framework and where necessary, a clarification of how international law principles apply to cyberspace should be elaborated. The negotiation of new international rules was not seen as a priority at the moment.

Gender Reporting

- Estimate the overall number of the participants present at the session: between 25 and 30

- Estimate the overall number of women present at the session: around 10

- To what extent did the session discuss gender equality and/or women's empowerment?
The session did not discuss gender equality in particular. But it did discuss the overall involvement of all actors (and genders) in cybersecurity issues and the need for capacity building initiatives in order to reach that goal.
- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion: There was no discussion on gender equality specifically.