IGF 2017 Reporting Template

Session Title: A Digital Geneva Convention to Protect Cyberspace

Date: Tuesday December 19th

Time: 10:40 – 12:10

Session Organizer: Microsoft and Diplo Foundation

Chair/Moderator: Duncan Hollis, Professor of Law, Temple Law School
(Online moderator) Kaja Ciglic, Director, Global Security Policy and Strategy, Microsoft
(Online moderator) Vladimir Radunovic, Director of Cybersecurity, Diplo Foundation

Rapporteur/Notetaker:
Jessica Zucker, Cybersecurity Strategist, Microsoft
Tereza Horejsova, Director of Project Development, Diplo Foundation

List of Speakers and their institutional affiliations:

- Paul Nicholas, Senior Director, Global Security Strategy and Diplomacy, Microsoft
- Ben Hiller, Cybersecurity Officer, Organization for Security and Cooperation of Europe (OSCE)
- Dr. Konstantinos Komaitis, Director of Public Policy, Internet Society
- Marilia Maciel, Digital Policy Senior Researcher, Diplo Foundation
- Elina Noor, Director of Foreign Policy and Security Studies, Institute of Strategic and International Studies
- Yvette Issar, Researcher, University of Geneva

Key Issues raised (1 sentence per issue):

- What does the cyber threat landscape look like today?
- How have international conversations on cybersecurity norms evolved over the years?
- Could a Digital Geneva Convention fill the gaps in the norms processes?
- What lessons can we learn from non-ICT fields in terms of when treaties were formed for other global governance problems?

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

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

Duncan Hollis opened the session by describing how there is widespread consensus that the current state of cybersecurity is unsustainable. There is a need for a cybersecurity framework to protect civilians in times of peace. According to Paul Nicholas, attacks in the last years have evolved substantially - now, more than 30 governments likely have offensive capabilities. Unlike traditional kinetic space, such as land, air and sea, cyberspace infrastructure is predominantly owned and operated by the private sector. However, the private sector has been unduly left out of the conversation, and governments cannot solve the existing challenges alone. Yvette Issar provided several examples of parallel global governance challenges from which we can draw lessons from and apply to cyberspace.

According to Dr. Konstantinos Komaitis, investments in cyber capabilities (offensive or defensive) will clearly continue in the coming years, therefore it is essential to clarify how international law applies to cyberspace. While international legal frameworks do exist to cyberspace, the application of such frameworks are ambiguous, with key questions remaining such as what constitutes a cyber-attack.

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

Ben Hiller offered that going forward there are two fundamental question: is there political will at the state level to engage and what happens if these regimes fail to deliver. International law breaks every day, and being realistic, we must consider that this would happen in the field of cybersecurity as well. In addition, there are a number of unresolved questions about how to drive progress forward: who manages the multistakeholder discourse? Will every company be sitting at the table? How do we implement such a multistakeholder process? What are the suitable platforms for this?

According to Komaitis and Marilia Maciel, the current process for deciding on these rules are done between states behind closed doors, with effected stakeholders expected to follow these decisions. However, we have seen from the failures of the UNGGE and continued cyber intrusions that these rules are not working. More inclusive processes need to proliferate, such as through a Digital Geneva Convention and parallel Tech Accord.

Elina Noor reminded that as we go forward, we must also consider what we mean by a rules-based order for cyberspace. The rules are being shaped by those countries with the strongest capabilities, yet the values they hold may differ from the ideals and governmental systems that other countries hold. The idea of protecting a specific type of ideal for a cybersecurity framework is not necessarily representative of the entire international community.

Gender Reporting

Estimate the overall number of the participants present at the session: 200

Estimate the overall number of women present at the session: 80

To what extent did the session discuss gender equality and/or women's empowerment? Discussions focused on the need to include all stakeholders in discussions around ensuring safety and stability in cyberspace.

If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion: There was agreement amongst participants that there needs to be full inclusion of all relevant stakeholders.