REPORT OF THE IGF 2017 MAIN SESSION

EMPOWERING GLOBAL COOPERATION ON CYBERSECURITY FOR SUSTAINABLE DEVELOPMENT & PEACE

Please click here for the Transcript (WE CANN'T FIND THE SCRIPT)

Please click [here](#) for the Video

1.0 Opening:

The main session was co-organized and co-moderators by Olusegun Olugbile, MAG Member and Juan Alfonso Fernández González, MAG Member respectively. Ambassador Frank Grütter, Head of the Division for Security Policy, Directorate of Political Affairs, Federal Department of Foreign Affairs, served as the Host Country Chair, while Ms. Lynn St Amour the Chair of the United Nations Internet Governance Forum Multistakeholders Advisory Group co-chaired the session.

Ms. Lynn St Amour introduced Ambassador Frank Grutter who gave an opening remarks welcoming the speakers and participants for the main session. The Ambassador highlighted the significance of the session in the light of major efforts being made by global stakeholders towards achieving a secure cyberspace.

2.0 Background Information

Since the inception of the IGF, Cybersecurity has been one of the key areas of concerns and discussions, with the Internet community stakeholders expressing grave concerns about the future of the Internet, its value for development, peace and preservation of our mutual interests in the cyberspace. The global economic and development agenda as enshrined in the resolution adopted by the General Assembly of the United Nations in 2015, *Transforming our world: the 2030 Agenda for Sustainable development*, continue to be under a serious threat from being achieved if the global actors decline to shape various commitments and ideas on global cooperation on cybersecurity and preservation of the stability of the Internet into global actions.

The existence of critical global cybersecurity issues have underscored the urgent need for a renewed multi-stakeholder dialogue on the security of cyberspace for peace and sustainable development. However, there have been various institutional frameworks for dealing with cooperation on cybersecurity, which are operating in silos, and are yet to be

translated into a meaningful global course of action. The IGF main session on cybersecurity is contributing further to a global multi-stakeholders dialogue stream that empowers Global Cooperation on Cybersecurity for Sustainable Development & Peace.

In this regards, the session built upon the previous efforts and outcomes of <u>IGF 2015</u> and <u>2016</u> main sessions on cybersecurity, the existing global initiatives such as <u>Global Commission on Stability of Cyberspace (GCSC 2017),</u> and the unfinished works of various global institutions and stakeholders including the UN Government Group of Expert in the context of Information Security,(UN-GGE2017).

3.0 Agenda with Key Policy Questions & Issues Discussed

The main session explored the following important issues and policy questions with speakers selected across diverse stakeholders groups.

Policy Question I:*The Best Practices Forum on Cybersecurity, organized within the IGF, this year focused on identifying how cybersecurity can help achieve the Sustainable Development Goals. What ties did the group establish between cybersecurity, and development?*
Speaker: Maarten Van Horenbeeck: *Director, Forum of Incident Response and Security Teams (FIRST)* United States of America Academia / Technical Community

Policy Question II: *What can be a development centred framework for cybersecurity?*
Speaker**:** Anita Gurumurthy *Executive Director, IT for Change,* India Civil society

Policy Question III: *Why is cybersecurity a human rights issue?*
Speaker: Valeria Betancourt *Manager, Communication and Information Policy Program, Association for Progressive Communications, APC,* Ecuador Civil society

Policy Question IV: *As perhaps the weakest link in the cybersecurity nexus, how can developing countries enhance global cooperation on cybersecurity for sustainable development & peace?*
Speaker: Jimson Olufuye *Chairman, Africa ICT Alliance (AfICTA)*, Nigeria Business sector

Policy Question V: *What are the African Challenges, including the research challenges with regards to cybersecurity?*

Speaker: Uche M Mbanaso, *Executive Director, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.* Academia / Technical Community

Policy Question VI: *How should government help achieve global cooperation on cybersecurity among different state actors in developing country?*

Speaker: Mohammed Tanimu Abdullahi, *Brigadier General,, Presidential Communication Command and Control Centre, Nigeria & Representative of National Security Adviser Nigeria.* Government

Policy Question VII: *How can we foster effective participation of civil society, private actors, tech community and academia in the global debate on international peace and security in Cyberspace?*

Speaker: Carmen Gonsalves Head International Cyber Policy, Ministry of Foreign Affairs, Netherlands, Government

Policy Question VIII: *What, in concrete terms, could the civil society do to support the norms for a peaceful cyberspace process?*

Speaker: Daniel Stauffacher *President, ICT4Peace Foundation*, Switzerland Civil society

Policy Question IX: What should be the role of the technology industry to keep the Internet safe and secure?

Speaker: Audrey Plonk, Senior Director, Global Cybersecurity and Internet Governance Policy, Intel Corporation United States of America, Business sector

Policy Question X : *In your opinion, what is the role of the United Nations and its intergovernmental agencies in the Global Cooperation on Cybersecurity for Sustainable Development & Peace?*

Speaker: Marco Obiso, *Cybersecurity Coordinator, International Telecommunications Union (ITU)* Geneva, Inter-governmental organizations

Policy Question XI: *What should we do to resume discussion on international information security issues under the UN auspices, and how to make it more practical and efficient?*

Speaker: Andrey Krutskikh Ambassador-at-Large, Special Representative of the President of the Russian Federation for International Cooperation in Information Security, Russia

Government

Policy Question XII: *The biennial Global Conference on Cyberspace began in London in 2011, being named the "London process". In your opinion, what role should the 'London Process' play towards empowering international cooperation on the security of cyberspace?*

Speaker: Sarah Taylor *Director, Cyber, National Security Directorate, Foreign & Commonwealth Office,* United Kingdom Government

Policy Question XIII: *You have chaired the Global Commission on Stability of Cyberspace since March 2017. What has the Commission done/achieved so far and how do you see the role of the Commission (in the context of the theme of this session).*

Speaker: Marina Kaljurand *Chair of the Global Commission on the Stability of Cyberspace,* Estonia Government

Policy Question XIV: *What are your views, from a disarmament, arms control and non-proliferation angle, on current challenges on ICT security issues and possible solutions?*

Speaker: Anja Kaspersen *Director, United Nations Office for Disarmament Affairs (UNODA) Geneva Branch* UNODA, Inter-governmental organizations.

Policy Question XV: Microsoft recently stated that the world needs a Digital Geneva Convention. Can you explain the elements contained in this proposal, and why it is important?

Speaker: Jan Neutze *Director of Cybersecurity, Microsoft Corporation, Belgium.* Business sector

Policy Question XVI: What can and should be done internationally to promote open, secure, resilient, stable and accessible cyberspace/use of ICTs, after the 2016/2017 GGE could not agree a consensus report?

Speaker: Marina Kaljurand, *Chair of the Global Commission on the Stability of Cyberspace*, Estonia Government

Policy Question XVII: *What obstacles do you appreciate for the adoption by the States of the recommendations of the Final Report of the Group of Governmental Experts in the Context of International Information Security that concluded its work in 2015?*

Speaker: Miguel Gutiérrez*General Director of the Security Office for Computer Networks, Ministry of Communications* Cuba, Government

Policy Question XVIII: *Cyber Security is a global challenge to be dealt with through cooperation. What kind of concept and approach that the international community should adopt when advancing international process of cyber security, with a view to enhance cooperation and safeguard peace and development of the cyber space?*

Speaker: Long Zhou*Coordinator for Cyber Affairs, Ministry of Foreign Affairs*, People's Republic of China, Government

Policy Question XIX: How can we ensure that the rule of law governs cyberspace?

Speaker: Carmen Gonsalves*Head International Cyber Policy, Ministry of Foreign Affairs,* Netherlands Government

Policy Question XX: How could we make international cyberspace more secure and stable bearing in mind that the global business is now thinking about "rules of the game" in ICT sphere?

Speaker: Andrey Krutskikh *Ambassador-at-Large, Special Representative of the President of the Russian Federation for International Cooperation in Information Security,* Russia, Government

Policy Question XXI: *In your opinion, what would be the most relevant elements to solve in order to reach a common understanding regarding the security of cyberspace?*

Speaker: Miguel Gutiérrez, *General Director of the Security Office for Computer Networks, Ministry of Communications* Cuba, Government

Policy Question XXII: *Microsoft also raised that there is a need to establish an international cyberattack attribution organization. Can you give some details on how this organization will be and function? How would we practically implement this as an international community?*

Speaker: Jan Neutze *Director of Cybersecurity, Microsoft Corporation*, Belgium, Business sector

Policy Question XXIII: *One of the biggest challenges with the multi-stakeholder model is that there are different perceptions and views on cybersecurity. What type of methods exists that can allow us all to work together and actually govern, even though responsibilities are so distinct?*

Speaker: Maarten Van Horenbeeck *Director, Forum of Incident Response and Security Teams (FIRST),* United States of America Academia / Technical Community.

Policy Question XXIV: *Are there other aspects of international cyber security that the civil society can help mitigate, take forward?*

Speaker: Daniel Stauffacher, President, ICT4Peace Foundation, Switzerland Civil society

Policy Question XXV: *As threats are global, there is some agreement that we need a global culture of cybersecurity in order to be fully effective at defending the internet. Is there a role for education providers in helping create this culture?*

Speaker: Uche M Mbanaso *Executive Director, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria* Academia / Technical Community

Policy Question XXVI: What challenges/barriers do you see to human rights based approaches to cybersecurity policy?

Speaker: Valeria Betancourt Manager, Communication and Information Policy Program, Association for Progressive Communications, APC Ecuador, Civil society

4.0 Summary of the Outcome:

i.   Cybersecurity and the preservation of a secure and reliable cyberspace are essential elements in the road towards sustainable development. Some pointed out that countries have different levels of preparedness to deal with cyber threats and cyber risks, and more efforts need to be focused on capacity building measures. It is important for countries to have institutions, strategies, and policies in place to tackle cybersecurity issues, but capacity development should also focus on the individual nations.

ii. Cybersecurity cannot be achieved by one stakeholder group on its own, and all stakeholders have roles and responsibilities. Participants warned that siloed approaches can lead to ineffective and counterproductive measures, and therefore, multistakeholder cooperation needs to be reinforced. Such cooperation carries challenges, one of them being related to the fact that there is no universally agreed definition of cybersecurity.

Hence, a global culture of cybersecurity could help to enhance mutual understanding among stakeholders on what, when, how can be done to ensure an open, secure, stable, and accessible cyberspace.

iii. While there was broad agreement that international law applies to cyberspace, calls were made for more efforts to clarify how it applies, and to identify whether there might be gaps in some areas that international law does not cover.

iv. Participants shared the view that cyberspace should be a place for peace, stability, and prosperity. International cooperation among states, some suggested in the framework of the UN, could contribute to avoiding a cyber arms race and militarisation of cyberspace.

v. Many agreed that existing norms related to responsible state behaviour in cyberspace – although not binding – can significantly contribute to enhancing cybersecurity and stability. Calls were made for more awareness raising about these norms, and more efforts to enhance their voluntary implementation.

vi. While some called for new international treaties or convention to encode rules, norms, and principles for cybersecurity and responsible state behaviour, others considered this premature and called for first identifying what could be the mechanisms that would allow meaningful engagement of all stakeholders in the development of rules. Moreover, questions were raised on the actual implementation and effectiveness of any potential future international agreement considering that there is still lack of clarity on how existing international law applies to the use of digital technologies by states.

vii. Participants shared views on the protection of the public core of the Internet while also calling for the extension of such protection to cover other critical elements, resources and components of the cyberspace.