IGF 2016 Workshop Report

Session Title	**How do Cybersecurity, Development and Governance interact? (WS 115)**
Date	9 December 2016
Time	9.00-10.30
Session Organizer	Kerry-Ann Barrett (Organization of American States), Carolin Weisser (Global Cyber Security Capacity Centre, University of Oxford), Carolyn Nguyen (Microsoft)
Chair/Moderator	Carolin Weisser
Rapporteur/Note taker	Carolin Weisser
List of Speakers and their institutional affiliations	Jorge Bejarano (Ministry for ICT Colombia) Belisario Contreras (Organization of American States) Natalija Gelvanovska (World Bank) Danil Kerimi (World Economic Forum) Carolyn Nguyen (Microsoft)
Key Issues raised (1 sentence per issue):	Cybersecurity capacity building plays a crucial role to achieve the SDGs and to ensure access and connectivity. The importance of the involvement of all stakeholder groups (including international and regional organisations, governments, other policy makers, as well as other implementers, the private sector and civil society) and the integration of cybersecurity capacity building components in all development projects. The need for a comprehensive approach, including both top-down and bottom-up, to enhance cybersecurity capacity across global and local spheres. There is a need for cybersecurity tools, models and frameworks to enable implementers to make cybersecurity capacity an integral part of development projects.
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	The WSIS review process showed that cybersecurity has become part of the debate. However, there is still a lack of understanding if not fear among policy makers, in particular from developing countries, on the role of issues such as cybersecurity, cyber threat, and cybercrime, and how to address them. An outcome of the WSIS process was the importance of multi-stakeholder approaches, as well as policy options and frameworks to tackle those issues.

	Currently, individual cybersecurity guidelines, regulations and national standards by governments create compliance issues that result in fragmentation of the internet. This goes against the idea of mainstreaming cybersecurity in developing countries to ensure connectivity and access, and help to achieve the SDGs and the Information Society. The Cybersecurity Capacity Maturity Model (CMM) from the Global Cyber Security Capacity Centre was presented as a good practice. The evidence-based framework aims to benchmark a country's cybersecurity capacity, and to enable policy makers to make better informed strategic investments for a more secure and inclusive cyberspace. The CMM looks at cybersecurity capacity through the five dimensions crucial to building a country's cybersecurity capacity: Cyber Security Policy and Strategy; Cyber Culture and Society; Cybersecurity Education, Training and Skills; Legal and Regulatory Frameworks; and Standards, Organisations, and Technologies. Since 2015, the CMM was deployed in over 45 countries around the world alongside key stakeholders, such as the World Bank, the Commonwealth Telecommunications Organisation, the International Telecommunication Union, and the Organization of American States (OAS). OAS provided an overview of a regional study based on the CMM and the crucial role of cybersecurity capacity-building for achieving the development goals of the member states. The OAS cybersecurity programme focuses on cybersecurity strategies and coordination of CSIRT, and the organisation tries to include as many stakeholders as possible to ensure that the development perspective. A national perspective on how cybersecurity capacity building efforts are linked to national development goals and integrated in the ICT development strategy was given by the panellist from Colombia. Besides environmental sustainability, economic development and social inclusion is the second pillar for the country's development approach - and ICTs are seen as the catalyst to achieving its objectives. The requirement for that is that citizens trust in the internet and cybersecurity therefore plays a key role in the digital policy. To the World Bank, Internet is perceived as a tool which contributes to the organisation's two overarching goals: to end extreme poverty and to promote shared prosperity. World Bank efforts are currently moving away from large infrastructure development projects to projects that connect rural areas with the focus is to bring people online. These kind of projects often have a lack of understanding for both the opportunities and the associated risk. That is the reason why cybersecurity capacity building is more and more integrated into these projects in terms

	of investments and capacity development plans. Only then the digital dividend can be realized, according to the World Bank. The World Economic Forum is traditionally interested in connecting the dots and the different players that are working together to achieve the objectives. They try to work directly with the leaders in business but also with academia and other stakeholders in these type of projects. In the past much effort went into sensitisation, however WEF have noticed a shift where organisations are proactively integrating cybersecurity capacity building into these projects and which is a development from sensitisation efforts. The Forum develops and provides tools in this regard.
Please describe the Discussions that took place during the workshop session: (3 paragraphs)	There was an overall agreement that cybersecurity capacity must be an integrated part of development initiatives at the inception phase as it goes hand in hand with the other issues in the Internet Governance domain such as *Connecting the Next Billion*, smart infrastructures, the digital economy, and human rights. Although it already can be observed that various actors take the nexus between Internet Governance, cybersecurity and development seriously, most of the panellists agree that there is still a lot to be done. One of the issues is the disconnect between different stakeholder groups, in particular between the development and cybersecurity worlds. The challenge for the OAS is, for instance, to quantify and provide indicators to convince decision makers in the governments for the relevance of integrating cybersecurity in the financial planning of development projects and to allocate resources for investment in cybersecurity. Many of the "traditional" development projects such as infrastructure and transportation which require large investments still do not contain cybersecurity elements although most of those projects have a link to ICT and the Internet. OAS is working through cooperation with the World Bank, Inter-American Development Bank, the Global Cyber Security Capacity Centre and Microsoft to provide evidence and indicators for the need of cybersecurity capacity building elements, including the above mentioned study. Another critical, but general issue is the lack of trust between stakeholder groups, which becomes more obvious during the review of cybercrime regulation which may cause some fragmentation. Also, as business continues to put out guidelines, users do not trust them. This relates to a challenge which was raised both from the panellists but also from the audience: the importance of awareness raising among users. Efforts require better coordination and involvement and inclusion of more stakeholders to cooperate on this issue. Whereas there were different opinions about if the cross-cutting relevance of cybersecurity capacity building is already efficient on

	the global policy level, all agreed that there is the need to provide solutions for the "how to" on both the policy and implementation level. Several good practice toolkits, frameworks and models for different issues for better securing the Internet were mentioned (see next section). Critical points which were raised is the risk that these models and frameworks are just copied and pasted. Also, a country may deem implementation all these recommendations challenging as the panellist from Colombia described in the case of the country's OECD membership process. However, the application process also provided the opportunity to bring the issue on the presidential agenda, to use the results for a new cybersecurity strategy and to enable cooperation agreement with other countries and the OAS. Lastly, Countries require recommendations on where/how to invest so cybersecurity needs are included in cross governmental financial planning.
Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	Creating policy options, guidelines, models: Those solutions should include certain cybersecurity norms, guidelines and baseline approaches (e.g. a set of vocabularies) which articulate output oriented advice. Participation by all stakeholders in creating these solutions and an open conversation between stakeholders should be encouraged, also those who have not been involved in the cybersecurity debate yet. There are already some useful examples, e.g. G7 Principles and Actions on Cyber (2016); G7 Fundamental Elements of Cybersecurity for the Financial Sectors (2016) and models such as the CMM. Those and other to-be-developed toolkits and the policy options developed must also go into the intersessional work including the BPF so that the outputs of the IGF go into the achievement of the SDGs. Fostering a global multi-stakeholder approach: Cybersecurity as part of it is a shared responsibility of all stakeholders. The IGF is a unique opportunity to have conversation about cybersecurity with the different stakeholders, in particular those who haven't participated in the debate yet, to build trust and to find solutions together. It was suggested that the IGF could also become the space to share experiences and talk about concrete actions. It is crucial to include the voices of practitioners and bottom-up approaches from the policy level to the implementation itself.