# IGF 2016 Workshop Report Template

| | |
|---|---|
| Session Title | **(WS132) - NetGov, Please Meet Cybernorms. Opening the debate.** |
| Date | 8 December 2016 |
| Time | 16:30 – 18:00 hrs. |
| Session Organizer | Madeline Carr, Duncan Hollis and Pablo Hinojosa |
| Chair/Moderator | Pablo Hinojosa |
| Rapporteur/Notetaker | Pablo Hinojosa |
| List of Speakers and their institutional affiliations | **Ms Marilia Maciel**, Digital Policy Senior Researcher, DiploFoundation<br>**Mr Duncan Hollis**, James E Beasley Professor of Law, Temple University School of Law<br>**Mr Henry Rõigas**, Researcher in Law and Policy Branch, NATO Cooperative Cyber Defence Centre of Excellence<br>**Dr Alejandro Pisanty**, Professor, National Autonomous University of Mexico (UNAM) and President, Internet Society, Chapter Mexico<br>**Mr Michael Walma**, Director and Cyber Foreign Policy Coordinator, Department of Foreign Affairs, Trade, and Development of Canada; Government Expert at the UN GGE.<br>**Ms Irene Poetranto**, Researcher and Communications Officer, Citizen Lab, Munk School of Global Affairs, University of Toronto<br>**Ms Izumi Okutani**, Policy Liaison, JPNIC<br>**Mr Paul Wilson**, Director General, APNIC; Member of the Advisory Board of Global Forum on Cyber Expertise (GFCE)<br>**Mr Juan Fernandez**, Senior Advisor, Ministry of Informatics and Communication of Cuba<br>**Mr Matthew Shears**, Head of Global Internet Policy and Human Rights, Center for Democracy and Technology<br>**Dr Anja Kovacs**, Director, Internet Democracy Project, India |
| Key Issues raised (1 sentence per issue): | There are different venues in which "cybernorms" are being discussed and propagated. Most of these discussions are dominated by State actors since they are held in a geopolitical or international security context.<br><br>The United Nations Group of Governmental Experts (UN GGE), for example, mainly focuses on international norms that aim to regulate State behavior with regard to cyber operations.<br><br>The session explored to what extent do the UN GGE government representatives actually look to other stakeholders for input or advice? It also asked if UN GGE recommendations can have consequences at the Internet operational level? Participants discussed the extent to which the technical community can support implementation of the GGE agreed norms and whether the IGF can serve as a platform to facilitate these engagements. |

| | |
|---|---|
| If there were presentations during the session, please provide a 1-paragraph summary for each Presentation | **Marilia Maciel**. In national security discussions, States protect their sovereignty. Maybe it's time for the security side to rethink where they place the individual in security discussions.<br><br>**Alejandro Pisanty**. The Internet has originally been based on trust by design and it has been able to survive in an environment where trust is not an assumption any more. A multistakeholder approach has worked well in solving Internet problems, but form has followed function so it varies by context. The Internet governance community tends to see CyberNorms as too high above their layers of the Internet. However, CyberNorms may provide useful specifications for the technical systems (such as the definition of an attack, whom to report one to, etc.) and may help keep some large-scale misconducts accountable.<br><br>**Duncan Hollis**. We might envision a more multistakeholder approach to the implementation of norms, monitoring whether States follow through what they agree to and figure out ways to build capacity, particularly at the technical level. Situational awareness is needed for both the IGF and UN GGE regarding their respective action plans.<br><br>**Henry Rõigas**. There is incomplete but somewhat overlapping focus between the UN GGE and IGF. It is important to build situational awareness: the Internet community should be aware of the knock-on effects if inter-State conflicts and States should be able to follow-up on those norms that affect non-State actors.<br><br>**Michael Walma**. The GGE should deal only with issues of peace and security, rather than with broader issues like cybercrime, cyberterrorism, or Internet Governance. For the latter, there are multistakeholder processes in place to discuss these topics.<br><br>**Irene Poetranto**. Attention needs to be placed not only on developing good norms, but also in researching about threatening and undemocratic norms such as Internet censorship practices, shutdowns and how they spread from one country to another.<br><br>**Izumi Okutani**. Network operators have norms as well. These are voluntary, publicly available, and open for comments from anyone interested. They can take the form of open collaboration, development of current best practices of bottom-up policy development processes.<br><br>**Paul Wilson**. The difference between a secure Internet and an insecure Internet has more to do with the skills and capacities of the people who are running, building, and maintaining it, than almost anything else. For the norms that are being talked about to be operational, there needs to be consideration of the effects and the |

| | |
|---|---|
| | side effects that they may have in the day-to-day operations of the networks.<br><br>**Juan Fernández**. Definitely there are linkages between cybernorms and Internet governance discussions, because they relate to the Internet and they talk about the same space in a way. We should try to find the common ground where these relationships could occur.<br><br>**Mathew Shears**. Asked to what extent the GGE looks to the technical community for responses, and vice versa.<br><br>**Anja Kovacs**. Cybersecurity and Internet governance discussions have not actually evolved far apart. Research by the Internet Democracy Project shows that in India, cybersecurity has been the main driver of much of the government stances taken in the Internet governance arena. Moreover, while related discussions play out in several different venues at the global level, disagreements spill over in many more venues, strongly affecting the work of civil society actors who are, however, excluded from participating in venues where these discussions are actually shaped. |
| Please describe the Discussions that took place during the workshop session: (3 paragraphs) | The session concluded that the IGF stakeholders might be able to help States to operationalize some of the norms being developed at the UN GGE, such as not targeting critical infrastructure or not having CERTs be the target of malicious activities. The speakers agreed that there could be a mutually constructive ways forward for the GGE to be more open and transparent and for Internet governance stakeholders to be more aware and involved in these discussions. |
| Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs) | The UN GGE will do well in being informed about the perspectives from the Internet Governance side, what uncertainties it brings to State level decisions.<br><br>A paper on what the gaps are, how to bridge them or how to structure collaboration between cybernorms and Internet governance discussions. Next meeting we should try to narow this gap.<br><br>To have a session at the IGF 2017 on the as yet unwritten 2017 UN GGE report. The sesión could be similar to the WSIS+10 Review session we had at the IGF 2015, with formal input into official government processes where everybody can contribute, keeping in mind that it will still be the governments who ultimately decide.<br><br>More proactive information sharing and creating room for other stakeholders to make observations. |

| | |
|---|---|
| | Promote convergence of global experts at the Global Conference on Cyberspace (GCCS).<br><br>States will have norms that will guide their behavior, but they don't have to be State-centric in operationalizing them entirely. The UN GGE should think how to involve the technical community, to think about what role the IGF and the IGF community do play in operationalizing these norms.<br><br>Some participants announced their intention to work together in order to perform work that amounts to a gap analysis between the perspectives from the two fields that may lead to a work program. |