IGF 2017 Reporting Template

- Session Title: International Cooperation between CERTs: technical diplomacy for cybersecurity?

- Date: 20 December 2017

- Time: 10:10am-11:40am

- Session Organizer: Pablo Hinojosa

- Chair/Moderator: Madeline Carr, Duncan Hollis, Pablo Hinojosa

- Rapporteur/Notetaker: Pablo Hinojosa

- List of Speakers and their institutional affiliations:

(in order of participation)

- Pablo Hinojosa, Strategic Engagement Director, APNIC
- Dr. Madeline Carr, Associate Professor of International Relations and Cyber Security, University College London
- Dr. Leonie Tanczer, Research Associate, University College London
- Adli Wahid, Senior Internet Security Specialist, APNIC. Board member of First.org
- Maarten Van Horenbeeck, Board member of First.org and Vice President, Security Engineering, Fastly.
- Louise Marie Hurel, Cybersecurity Project Coordinator, Igarapé Institute
- Duncan Hollis, Associate Dean for Academic Affairs & Professor of Law, Temple University School of Law
- Karsten Diethelm Geier, Head of Cyber Policy Coordination Staff, Federal Foreign Office, Germany
- Tobias Feakin, Ambassador for Cyber Affairs, Australia
- Gavin Willis, National Cyber Security Centre, UK
- Jan Neutze, Director of Cybersecurity Policy, Microsoft
- Elina Noor, Director, Foreign Policy & Security Studies, Institute of Strategic and International Studies (ISIS), Malaysia
- (remote) Camino Kavanagh, Visiting Fellow, Dept. War Studies, King's College London

- Key Issues raised (1 sentence per issue):

- In the last 30 years, CERTs/CSIRTs (hereafter referred as CERTs) have developed and grown in many different shapes and configurations. Most of them are not related to governments or national interests.
- The establishment of CERTs has become an indicator of cybersecurity development and maturity and many governments have sought to institutionalize CERTs as part of their national cybersecurity mechanisms.
- The performance of national CERTs is likely to be judged on how well the national networks are defended. However, the distributed nature of the Internet makes it very difficult to contain damages within national borders.
- As governments may increase regulation and oversight in the CERT space, it is crucial to preserve the voluntary information exchanges and the trust that has been earned through collaboration.

- CERTs cooperate, share information and maintain trust, even in difficult political contexts. Some academic researchers consider CERTs as inadvertent diplomatic actors, similar to the way that scientists have long been able to collaborate across borders.
- Alternative to the view of CERTs as diplomatic actors, is the view that official cyber diplomats, representing governments, only come into play at a late phase, when an incident has escalated to a point where the CERTs cannot respond, that is, when international peace and security are at risk.
- Political contacts and/or institutions at a governmental level cannot replace CERT work. In fact, most incidents are being resolved at the technical level without government interference.
- As cybersecurity concerns have grown, CERTs have become a component of the geopolitics of cybersecurity. Increased government interventions can affect well established networks of trust and undermine the work of CERTs.
- Political decisions should not prevent CERTs from resolving incidents. It is important that CERTs can respond quickly to make sure damages can be contained and not distribute further in the Internet ecosystem.
- The role of cyber diplomacy (as practiced by government representatives) is not to prohibit the use of ICTs in political conflict. It is to avoid inadvertently prompting an international conflict by accidental provocations in cyber space.
- For CERTs to work effectively, they cannot and should not be politicized. CERTs play an important role as first responders. They need to be able to function without technical or political interference.
- For the last several years CERTs have become subjects of norm making processes. Such is the case of the UNGGE. The latter agreed in 2015 on non-binding norms of responsible state behaviour, including not conducting or knowingly supporting activities to harm CERTs or using CERTs to engage in malicious international activities. The idea behind these norms is to protect the work CERTs are doing and to prevent them from being instrumentalized by the governments.
- However, there is little awareness of the UNGGE normative process within the CERT community or if there are any efforts underway in the implementation of those norms.
- In some countries, national CERTs play an important role in track 1.5 and track 2 diplomacy, particularly in bilateral settings. CERTs have become part of the diplomatic toolkit to assist governments with information sharing to fight cybercrime and in building linkages between international law and norms and how they relate to operational issues.
- However, other track 2 settings have not been successful in trying to merge the conversation between the technical and the policy communities, mostly because of the difficulty to find trusted points of contact in the policy arena.
- Cybersecurity is a shared concern and responsibility. Actors such at CERTs, especially national ones, are part of a political dimension. We, thus, need them to look at CERTs as part of a cybersecurity governance ecosystem, without undermining their technical relevance and independence.

- 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):

- Because the CERT community is very much focused on responding to incidents and solving cybersecurity problems, they do not perceive themselves as cyber diplomats. However, the international political community is increasingly referring to CERTs in strategies, proposed codes of conduct and coordination documents. The CERT community may not be fully aware of the extent to which they are becoming integrated into global politics.
- By analysing differences in cooperation, information sharing and trust protocols of the CERT and the diplomatic communities, this workshop raised awareness about both actors and reduced the level of disconnect and miscommunication between them.

- More engagement and shared understanding is needed to concentrate on positive impacts rather than negative influences that ultimately undermine global cybersecurity efforts.

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

- Whether CERTs can inform the processes that are needed for international cyberattack attribution. While CERTs have certain technical capabilities on this front, attribution of cyber-attacks to states is a highly political process. There are no standard methodologies in place, nor common thresholds to determine attribution. Governments could benefit to leverage CERT expertise on this front, but there are also significant risks that may affect the CERTs ability to cooperate with other governments who may not support the political process.
- Whether CERTs can initiate and play a relevant role in discussions with governments on some form of code of conduct or similar, for CERTs to remain independent, prevent harming each other and enhance response capabilities. Specifically, discussions on allowing CERTs to operate outside of sanctions regimes is important.
- Governments should engage with the CERTs and their regional and global associations, such as the Forum of Incident Response and Security Teams (FIRST), to determine how to best operationalise the norms recommended by the 2015 UNGGE report.

Gender Reporting

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

Around 110 pax.

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

50 pax.

- To what extent did the session discuss gender equality and/or women's empowerment?

n/a

- If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion:

- The list of speakers was big and quite diverse in terms of gender, stakeholder group and geographic representation.