IGF 2021: Workshop Proposal

Title	**One click to attack critical infrastructure. What can we do?**
Description	Two-part workshop that will discuss various elements of critical infrastructure protection (CIP) in a moderated panel discussion: 1. The first part will focus on national approaches and existing good practices to CIP, also touching on the global processes/negotiations taking place within the UN First Committee. 2. The second part will explore opportunities for creating a 'UN cyber emergency phone book' – mechanisms for a global incident response in the event of cross-border cyberattacks on CI. This will include discussion of the takeaways from the 2021 consensus OEWG report and, in particular, the recommendation on nominating national points of contact (PoC).
Desired outcomes	Conceptualization of key elements for ensuring critical infrastructure protection, an incident response policy, and identification of potential challenges and action items for the global community as a result of the two discussions involving experts and leaders representing different stakeholder groups and regions.
Format	Hybrid (details to be provided by the IGF Secretariat in the coming weeks): both online and on site in Katowice, Poland (IGF 2021 will be held on December 6-10, 2021)
Platform	Zoom – for those joining remotely
Agenda/Program	**Roundtable panel discussions in two parts:** **I. Conceptualizing a CI protection policy framework [45 mins]** *While protection of CI is a prerogative of states, including the formulation of what CI is, they are not the only ones operating in this field. A large portion of CI is owned and/or managed by the private sector. In the event of a cyberattack on CI, what's the recommended course of action? As the private sector has a responsibility to protect, what is it expected to do and not to do? What are the existing good practices and approaches to protecting CI? What are the takeaways from the 2021 consensus UN OEWG report for the global community?* Before the discussion, there will be an online quiz consisting of 3-4 questions to see how aware the participants are of existing good practices. • **Speaker 1:** Ambassador Regine Grienberger, German Federal Foreign Office (Government, Western European Group) (confirmed)

- **Speaker 2**: Mr. David Koh, Cyber Security Agency of Singapore (Government, Asia-Pacific Group)
- **Speaker 3**: Ms. Johanna Weaver, Australian Department of Foreign Affairs and Trade (Government, Asia-Pacific Group) (confirmed)
- **Speaker 4**: Ambassador Nadine Olivieri Lozano, Swiss Federal Department of Foreign Affairs (Government, Western European Group)
- **Moderator**: Ms. Anastasiya Kazakova (Private Sector, Eastern Europe Group)

II. Exploring opportunities for a 'UN cyber emergency phone book' [45 mins]

Where a cyberattack affects CI in several jurisdictions, is cross-border cooperation possible and how? Is a 'UN cyber emergency phone book' possible? If not, why not? If an affected state doesn't have the capability to respond and protect itself, who should it approach for help? What does the UN cyber stability framework suggest doing? What can be done to achieve stronger cooperation between CERTs/CSIRTs? And how can the neutrality of CERTs/CSIRTs be ensured during a cyber-crisis?

- **Speaker 1**: Mr. Serge Droz, FIRST (Intergovernmental) (confirmed)
- **Speaker 2**: Ambassador Henri Verdier, French Ministry for Europe and Foreign Affairs (Government, Western European Group) (confirmed)
- **Speaker 3:** Mr. Pierre Delcher, GReAT Kaspersky (Public Sector, Western European Group) (confirmed)
- **Speaker 4**: Mr. Neil Walsh, UNDOC (Intergovernmental) (confirmed)
- **Moderator**: Ms. Anastasiya Kazakova (Private Sector, Eastern European Group)