Invitation

Operationalizing a Global Database of Cyber Incidents – Successes, Challenges and Potential Way ahead at UN-Level?

Thursday, 7 March 2024 at 13:15 hours
German House
871 / 873 1st Avenue, New York

As set out in its resolution 75/240, the General Assembly recommended that the OEWG continue “to study, with a view to promoting common understandings of existing and potential threats in the sphere of information security, interalia, data security, and possible cooperative measures to prevent and counter such threats.” At this stage of the OEWG a proposal is being discussed to establish a non-attribution UN-run cyber threat repository, that members can voluntarily and regularly update in the face of the constantly evolving and diversifying cyber threats – this idea has most notably been advanced by Kenya and has resonated with many delegations.

Denmark and Germany would like to contribute to ongoing OEWG deliberations by presenting the European Repository of Cyber Incidents as an already existing platform established and maintained by independent research institutions. The European Repository of Cyber Incidents is conceptualized as a centralized and accessible platform for cyber threat information sharing and facilitation of informed responses to cyber threat attacks, indicators of compromise and where possible best practices that articulate how states have mitigated such threats. To jointly discuss how such a platform could contribute to cybersecurity and cyberstability at UN-level, Denmark and Germany would like to invite you to explore existing best practices and lessons learnt.

Experts of the European Repository of Cyber Incidents (www.eurepoc.eu) will be joining us for the 7th substantive session of the OEWG in New York to share their experiences of hosting a fully open-access data base of publicly known cyber incidents and continuously updating it. The European Repository of Cyber Incidents is a politically independent research consortium dedicated to providing evidence-based scientific analysis of cyber incidents for a fact-based understanding of the current cyber threat environment. Its resources include user-specific, reliable data based on an interdisciplinary research perspective. Building on this interdisciplinary data-driven research conducted by EuRepoC jointly with representatives from other member states, regional organizations and experts in the field, this side-event is eager to explore the following guiding questions among others:

- Which opportunities, challenges and lessons learnt can be drawn from operationalizing an open-access data base of publicly known cyber incidents with a particular political and increasingly often socio-economic relevance?
- How can state, commercial, and academic actors, such as EuRepoC, cooperate effectively to create the most comprehensive cyber conflict situation report possible?
- To what extent does the European repository of cyber incidents inform global stakeholders, but also the general public, about the current cyber threat environment and which conclusions can be drawn for cyber diplomacy about it?
- How could a global repository of cyber incidents at UN-level look like and be operationalized? What characteristics should it have (technical vs. non-technical information) in order to bring maximum benefit to the various stakeholders including global cyber diplomacy?
- What can we learn from existing threat intelligence platforms? Their potential and limitations?
We hope you will be able to join us for a timely discussion and lunch. Please note that seats are limited and RSVP to ks-ca-ext-gtz@auswaertiges-amt.de.