Responding to Cyber Crises and Building Accountability in Incident Response

OEWG Side Event

Date: Monday, 11 December 2023, 1315 - 1445 pm
Location: Permanent Mission of Estonia to the UN
Three Dag Hammarskjöld Plaza, 6th Floor, 305 East 47th Street, New York, N.Y. 10017

Organisers and Co-sponsors: Germany, RUSI, Estonia, UNIDIR, Montenegro and Kenya

All governments are faced with the growing challenge and need to respond to an evolving set of cyber incidents. Large scale or highly disruptive incidents can often (i) put to the test the existing understandings of malicious/unacceptable cyber behaviour, (ii) they can also trigger, challenge, or consolidate frameworks/institutions and (iii) highlight the shortcomings of coordination or lack of capacities to respond.

Part of the discussion on accountability has focussed on enhancing deterrents to malicious behaviour and, in many ways, raising the expectation of states being able to *technically* attribute specific malicious actors/behaviours with the aim of holding them accountable for such acts, especially for highly sensitive targets such as critical infrastructures. Technical attribution, while important, is one 'tool' in the toolbox for enhancing responsible cyber behaviour.

Recognising that while all technical attribution relies on incident response, not all incident response processes result in technical attribution, *Germany, the Royal United Services Institute (RUSI), Estonia, the United Nations Institute for Disarmament Research (UNIDIR), Montenegro and Kenya* are convening this side event to discuss accountability in incident response. The purpose of event is to bring governments together for a dialogue on ***how cyber crises can help us better identify the lessons learned and blockers for accountability in incident response*** and help advance a practice-oriented understanding of responsible cyber behaviour.

The processes through which states respond to malicious cyber activities, the capacities available, the frameworks in place, and the institutions involved in these processes vary. What is more, the political and economic incentives for technically attributing or determining unacceptable behaviours domestically and the development/implementation of national incident response procedures such as incident/risk categorisation also vary. Nonetheless, states can take proactive and reactive measures to enhance accountability in incident response (and, whenever desirable/possible, technical attribution) – all of which relate to the implementation of a series of norms within the existing framework for responsible state behaviour (i.e. 13(d), 13(j) or 13(h))

The sixth substantive meeting of the Open-Ended Working Group on the Security in and of ICTs particularly provides the opportunity to listen and learn from countries' practical experiences in dealing with emerging threats. The objective of this lunchtime workshop is to foster a context-sensitive discussion on the topic with the aim of providing further guidance on the global agreement

on the framework of responsible state behaviour in cyberspace while taking into account different national/regional and capacity realities.

It will do so by:

- Inviting governments to share their experiences of how they responded to malicious cyber activities and cyber crises;
- Inquiring about the frameworks, processes linked to incident response and crisis mitigation;
- Understanding how and under which conditions technical attribution has or not been conducted;
- Drawing from those practical experiences to have greater understanding on norms implementation.

Participants are expected to come prepared for an active discussion and share their experiences on the challenges related to incident management and technical attribution as well as in devising processes and procedures for establishing accountability for malicious activities in cyberspace.

The discussions will inform the development of a workshop report, which will be shared with Member States. The side event is part of RUSI's ongoing project on Responsible Cyber Behaviour, which seeks to advance the mapping of practical understandings of responsible state behaviour in cyberspace across different regions and the findings of the event will help inform the research.

For any additional queries please contact **Lilian Georgieva-Weiche**, German Federal Foreign Office (ks-ca-ext-gtz@auswaertiges-amt.de) and **Louise Marie Hurel**, RUSI (LouiseH@rusi.org). Light lunch will be provided.

AGENDA

1315-1330	**Arrivals**
1330-1340	**Welcome remarks** *John Reyels | Head of Cyber Policy Coordination Staff, German Federal Foreign Office* *Kristel Lõuk | Deputy Permanent Representative of Estonia to the United Nations*
1340-1410	**Learning and dealing with cyber crises: unacceptable behaviour for whom and when?** States will share their experiences in responding to large scale incidents, their incident management procedures/learnings and/or their decision to technically attribute or not. The objective of this section will be to map a spectrum of postures on incident response and attribution by sharing specific cases and thus, understanding, based on concrete examples, what is desirable and achievable in terms of accountability for countries across the developed-developing spectrum. **Guiding questions**:

	• Based on national experiences with large-scale incidents, what were the key enablers for effective incident mitigation? • Conversely, what would you say were the main blockers and how have/could they be addressed? • Even if *technical* attribution is not desirable, could you provide additional examples of unacceptable behaviours resulting from crises responses?
1410-1440	**<u>Practical responses to enhance accountability in incident response</u>** Incident response and attribution, more specifically, rely on at least three core pillars: evidence collection, legal analysis, and decision-making and communication.[1] In the second section we will be discussing existing the connection between those practical experiences and norms. Asking participants to contribute to the links between frameworks for accountability in incident response and the implementation of specific norms. **Guiding questions**: • Based on your national experience what do you think States should be accountable for, to whom and why? • How can accountability in incident response provide further guidance on the operationalisation of existing norms? • Could you share examples of how you think States can contribute to and enhance accountability of States and malicious actors in cyberspace? What can the OEWG or other forums/mechanisms support this discussion?
1440-1445	**Concluding remarks, takeaways, and next steps** *Louise Marie Hurel, RUSI*