Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

WS #190 Securing critical infrastructure in cyber: Who and how?

Internet Governance Forum (IGF)

CONCEPT NOTE

18 December 2024

13:45 - 15:15 (Saudi Arabia local time)

Description

In an era where interdependencies stretch across borders and hybrid threats blur the lines between cyber and physical domains, a critical question emerges: Are states and key stakeholders truly prepared to protect critical infrastructure (CI)?

With the shifting nature of cyber threats, how can relationships between public and private actors evolve to better protect CI in both peacetime and conflict? How do advances in technology, from AI to IoT, influence strategies for critical infrastructure protection (CIP), and should there be a baseline of international cybersecurity standards for CIP?

Further, as the agreed UN cyber norms gain traction, what role can they play in approaching CIP? Is there sufficient clarity in the responsibilities of non-state stakeholders, and how might these stakeholders support states in fostering responsible behaviour in cyberspace?

On 18 December at the UN IGF, the *Geneva Dialogue on Responsible Behaviour in Cyberspace* will address these concerns in a multistakeholder approach, engaging representatives from the private sector, academia, civil society, and technical community for a regular dialogue. Established by Switzerland in 2018 and implemented by DiploFoundation with support of others, the Dialogue maps the roles and responsibilities of various actors in the implementation of agreed cyber norms and thus contributes to stability and security in cyberspace.

The outcomes are published in the *Geneva Manual*, offering a comprehensive guidance on non-state actors' implementation of the normative framework agreed by states, in the context of the UN GGE/OEWG. The session will bring together actors, including those from the Global South, to discuss the issues identified above, provided also in a format of a scenario-based discussion, i.e. simulation exercise. The insights gathered during the session will contribute to the forthcoming chapter of the Geneva Manual, focusing on the implementation of CIP related cyber norms and confidence-building measures (CBMs).

Participants will also learn best practices, develop ideas, and network with thought leaders in the field of cyber policy for critical infrastructure.

Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Format

The session invites public sector policymakers, critical infrastructure operators, cybersecurity professionals, compliance professionals, academics, civil society, and experts from the cybersecurity and cyber diplomacy community.

https://intgovforum.org/en/content/igf-2024-ws-190-securing-critical-infrastructure-in-cyber-who-and-how

Location

Workshop room 4

Speakers and facilitators:

- **Bushra AlBlooshi,** Director of Cybersecurity Governance Risk Management Department, Dubai Electronic Security Center
- **Kazuo Noguchi**, Senior Manager R&D, Hitachi America
- **Nicolas Grunder** ,Global Lead Counsel Digital, Data & Cyber, ABB
- **Kaleem Usmani,** Head of the CERT-MU, Mauritius
- **Klée Aiken**, Director, Community & Capacity Building, the Forum of Incident Response and Security Teams (FIRST)
- **Melanie Kolbe-Guyot**, Head of Digital Policy, C4DT - EPFL
- **Vladimir Radunović,** Director, E-diplomacy and Cybersecurity Programmes, DiploFoundation
- **Anastasiya Kazakova,** Cyber Diplomacy Knowledge Fellow, DiploFoundation

Programme

13:45 - 13:50	**Welcome address** • **Vladimir Radunović,** DiploFoundation • **Thomas Schneider,** Swiss Federal Office of Communications (OFCOM)
13:50 - 14:00	**Geneva Manual on Responsible Behaviour in Cyberspace** • **Anastasiya Kazakova,** DiploFoundation
14:00- 14:40	**Geneva Manual tabletop exercise: Defining the minimum cybersecurity measures for critical infrastructure protection (CIP)** **Facilitated by Vladimir Radunović,** DiploFoundation and **Melanie Kolbe-Guyot**, Head of Digital Policy, C4DT - EPFL
14:40 - 15:10	**Exchange of views and roundtable** **Guiding questions:** 1. How can we effectively protect critical infrastructure, facilities, and assets that have national, regional or international impact? What measures should be implemented, and which stakeholders need to be engaged?

	2. What is the role of cyber norms and CBMs when it comes to the protection of CI? Does their voluntary nature have an impact on the protection of CI? 3. Is it reasonable to expect cyber operations to avoid targeting critical infrastructure, or is that an unrealistic expectation? 4. How can confidence-building measures (CBMs) be strengthened to ensure better coordination in responding to incidents and cyber threats affecting CI? 5. How do we establish accountability for harm caused by threats to critical infrastructure, especially when agreed-upon norms are violated? **Facilitated by Vladimir Radunović,** DiploFoundation and **Melanie Kolbe-Guyot**, Head of Digital Policy, C4DT - EPFL
15:10 - 15:15	**Concluding remarks**