20 May 2023

CONCEPT NOTE

IGF KYOTO 2023 – "Shaping Internet Governance in Times of Conflict"

A joint side-event organized by the German FFO, Access Now, CyberPeaceInstitute and ICANN [and additional partners]

Background:

While the world has been shocked by the physical devastation in Ukraine, a hidden part of the conflict is underway in cyberspace. The year 2025, the 20th anniversary of WSIS and the year the IGF's current mandate expires, will be a decisive moment for internet governance. A likely defining parameter in these discussions of "who runs the internet" will be perceptions on different approaches to advancing peace, stability, and security while maintaining openness and respect for human rights and sustainable development. Strengthening the multi-stakeholder governance model of the internet and supporting a more positive and inclusive digital future is now more crucial than ever.

Against this backdrop, the panel "**Shaping Internet Governance in Times of Conflict**" – co-hosted by the German Federal Foreign Office, Access Now, CyberPeaceInstitute and ICANN – explores the reality of current cyber conflicts, their effects on civilians, the need to ensure free, open, and secure access to the Internet in conflict areas and the consequences for internet governance. A core goal of this event will be to identify avenues for effectively **future-proofing and strengthening the IGF, its mandate and governance architecture** and to discuss policies for effective multi-stakeholder governance of the internet in a world where conflicts increasingly stretch from the physical to the cyber realms and questions of accountability arise.

The side-event will bring together **experts from governments, civil society, the private sector and those directly affected from areas of armed conflict**.

The panel will explore the following themes:

At the governance level:

- Understand the **nature, challenges and actors** (often private) **of current armed conflicts** and how their dynamics interact in the online realm. What are present and potential **de-stabilizing spillover effects** beyond belligerent countries?
- Present **real-world examples** of physical-cyber conflict dynamics, with examples focusing on occupation/control, spyware, internet shutdowns and sanctions as well as the impacts they have on affected people/civilians/communities.
- Discuss **norms, best practices and policies** for effective internet governance in interstate conflict to prevent internet fragmentation/"splinternet" and censorship. What can we learn from civil society and the private sector in preventing and managing internet restrictions aside from government action? Which stakeholders need to be involved in effective internet governance? How can we balance competing interests, such as fighting disinformation or restricting dissemination of state-sponsored propaganda, hate speech and incitement to violence, while providing citizens free access to information?
- Consider the **future of the internet** and the **future of IGF**: how to ensure the openness of the internet, especially in areas under occupation? How do we ensure data rights and privacy are protected under international law, especially in occupied areas? How can the existing IGF mandate be reinforced and reflected in the GDC process in view of strengthening internet governance through this emerging global pact?

At the practical level:

- Explore which practical tools are needed to respond to war-time needs of civilians, victims;
- Establish **fora and technical tools** for short-notice **incident response -** building on **lessons-learned and showcasing practical efforts** of **dedicated civil society organizations**, such as cyberattack monitoring or internet shutdown trackers.

Implementation & Format:

The side event will be hosted at the margins of the IGF in Kyoto 2023. It will gather results of a **chain of events throughout 2023,** looking into **digital governance in contexts of conflict**, starting with the **Stockholm Conference** in May ("tech in conflict"), the **RightsCon Summit** in Costa Rica (dedicated event on "AI abuses by authoritarian regimes on human rights") and the Berlin-based "**Shaping Cyber Security Conference**" in June and, finally, leading up to the **IGF in Kyoto** in October (internet governance in times of conflict).

The event will be held under the **Chatham House** rule with the participation of stakeholders from academia, governments, civil society, and industry. The session will include **interactive elements** to encourage exchange between all stakeholders in the discussions.

Potential Partners:

The aim is to ensure **high-level government representation**, for example, by co-hosting the event with **like-minded partners of the FOC** or countries that have been particularly dedicated / committed to contributing to the **Global Digital Compact consultations** on **internet governance** and **human rights online**. Also, high **level participation of the Tech Sector** should be aimed at, possibly by inviting Amazon or, for example, the Slovak company, ESET.