Geneva Dialogue
ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Best Practice Forum

Securing Access to the Internet and Protecting Core Internet Resources in Contexts of Conflict and Crises

CONTRIBUTION

About Geneva Dialogue on Responsible Behaviour in Cyberspace

The *Geneva Dialogue on Responsible Behaviour in Cyberspace* (Geneva Dialogue) is an international process established in 2018 to map the roles and responsibilities of non-state stakeholders – private sector, civil society, academia, and technical community – in contributing to greater security and stability in cyberspace. It is led by the Swiss Federal Department of Foreign Affairs (FDFA) and implemented by DiploFoundation, with support of the Republic and State of Geneva, C4DT, Swisscom and UBS.

In 2020–2021, the Geneva Dialogue concentrated on the private sector's role in addressing vulnerabilities in digital products and ICTs. The *output report* presents insights from ongoing discussions with private sector partners and includes their written submissions. The document also sets out the definitions related to secure design that have been agreed upon by the partners and highlights some of the best practices that the partners are following to build more secure products and minimise ICT vulnerabilities.

In 2023, the Geneva Dialogue launched a new phase to clarify the roles and responsibilities of relevant non-state stakeholders from the private sector, academia, civil society, and technical community (including open-source community) in the implementation of the agreed cyber norms. The first round focused on discussing the agreed cyber norms related to ICT supply chain security and responsible reporting of ICT vulnerabilities.

Practically the Geneva Dialogue organises regular consultations with more than 69 organisations representing different stakeholder groups to document their interpretation of the agreed norms and views on their implementation, while also gathering best practices that can inspire the international community. These findings are published in the *Geneva Manual on Responsible Behaviour in Cyberspace*.

During the 2024–2025 phase, the Geneva Dialogue focuses on analysing the implementation of agreed cyber norms and confidence-building measures (CBMs) related to critical infrastructure protection (CIP). The outcomes of these discussions are reflected in the *second chapter of the Geneva Manual*, which captures feedback from the multistakeholder community on the implementation of these norms and CBMs.

This contribution shares relevant findings from our work, with the aim of providing additional multistakeholder input to support the efforts of the BPF.

1. Feedback on the draft problem statement

The problem statement proposed by the BPF—*calling for clarification of the roles and responsibilities of the multistakeholder Internet community in securing core Internet resources and ensuring civilian access to the Internet during conflicts and crises*—resonates with discussions in the Geneva Dialogue, particularly regarding the implementation of agreed cyber norms and CBMs related to critical infrastructure protection.

The *Geneva Manual's second chapter*, developed through inputs from over 69 global stakeholders, highlights the growing urgency of addressing cross-jurisdictional interdependencies that underpin the general availability and integrity of Internet infrastructure. As noted in *Key Message #1*, "*more international efforts are required to*

*understand and protect cross-jurisdictional interdependencies in some CI sectors with regional and international impac*t."

In this context, discussions within the Dialogue have shown that defining 'core Internet resources' remains contested and context-dependent. Some stakeholders view core resources in strictly technical terms—such as the DNS, IP addressing, root zone management, and routing infrastructure—while others take a broader approach, encompassing the socio-technical systems and institutional arrangements that support Internet continuity and resilience. This includes software supply chains, cloud and data service providers, and the underlying dependencies between CI sectors.

The Manual also underscored that ambiguity in defining these resources may hinder the operationalisation of the agreed cyber norms. Without a clearer mapping of interdependencies, it may be difficult to establish shared expectations or coordinate responses during incidents that impact Internet accessibility—particularly in humanitarian or conflict settings.

The Geneva Manual outlines practical actions to address these challenges. It recommends that "*relevant stakeholders (CI operators/owners, product vendors and service providers, cybersecurity researchers and incident response experts, OSS experts, NGOs and academia)*" assist states in identifying interconnected assets, systems, and networks. This effort should also involve "*analysis of cause-and-effect relationships and possible cascading failures*".

Finally, the Dialogue's discussions reaffirm that ensuring civilian access to the Internet during crises requires a shared understanding of which infrastructures are essential, and how they are governed across jurisdictions. This demands not just conceptual clarity, but also deeper cooperation among public and private actors—grounded in transparency, trust, and a common commitment to protecting the digital foundations of society.

Building on this, the current framing addresses an important issue but could be further strengthened through the following clarifications:

- **Acknowledge the plurality of interpretations of "core Internet resources"** – While providing a fixed definition may be challenging, it would be helpful to recognise the varying understandings among stakeholder communities. This includes both narrowly technical components (e.g. DNS, IP routing) and broader socio-technical systems essential for Internet continuity.
- **Specify stakeholder categories** – The phrase *"multistakeholder Internet community"* would benefit from greater precision. Referring explicitly to key actors—such as service providers, technical operators, civil society, academia, and the open-source community—can help clarify expectations and responsibilities.
- **Highlight cross-jurisdictional interdependencies** – Many core Internet resources are inherently transboundary. Disruptions in one part of the infrastructure can have regional or even global consequences. Acknowledging these interdependencies is essential to understanding the scale and nature of shared risks.
- **Clarify the scope of "civilian access"** – The current phrasing could be expanded to reflect the importance of maintaining access to essential digital services and communications, particularly in humanitarian contexts and during armed conflict.
- **Reframe "clarify roles" to emphasise coordination and shared responsibility** – Rather than suggesting static role assignments, the statement could promote coordinated action and flexible collaboration among stakeholders, reflecting the distributed nature of Internet governance and incident response.

2. Main challenges

Ensuring the protection of core Internet infrastructure and maintaining civilian access during crises and armed conflicts involves navigating a range of complex challenges. Drawing from

the multistakeholder consultations of the Geneva Dialogue and the findings of Chapter 2 of the Geneva Manual, the key challenges include (but not limited to):

- **Cross-jurisdictional interdependencies and cascading risks**. The Internet's global nature means that critical infrastructure often spans multiple jurisdictions. Mapping interdependencies between sectors, countries, and systems remains insufficient, making it difficult to predict and contain cascading failures during crises.
- **Fragmented responsibilities and coordination gaps.** With responsibilities distributed across governments, private sector entities, and technical operators, crises often expose unclear lines of accountability and the absence of pre-established coordination mechanisms—particularly when infrastructure is privately operated or governed by multiple jurisdictions.
- **Geopolitical tensions and restrictions on technical cooperation**. As outlined in *Message #5 of the Geneva Manual, 2nd chapter,* cybersecurity researchers, incident response teams, and other technical experts increasingly face restrictions on cross-border cooperation due to sanctions, export controls, and national security laws. These constraints hinder the exchange of threat intelligence and incident data, fragment the global response ecosystem, and weaken collective defence capabilities. Furthermore, the rising politicisation of cyberspace undermines the perceived neutrality and operational effectiveness of the technical community. Restrictions on engagement with counterparts in sanctioned or adversarial jurisdictions prevent experts from addressing shared threats—such as ransomware or vulnerabilities in widely used technologies—thus increasing risks to critical infrastructure globally.
- **Targeting and disruption during conflict.** In conflict scenarios, digital infrastructure may be targeted or affected to disrupt communications, inflict economic harm, or suppress access to information. These include attacks on telecom providers, Internet exchanges, submarine cables, and cloud services.

3. Applicable norms, agreements, and processes

Several agreed cyber norms are directly relevant to the protection of core Internet infrastructure and ensuring civilian access during crises. Notably, these are UN GGE norms (F, G, H, I and J) and confidence-building measures, as well as regional frameworks such as OSCE confidence-building measures.

4. Operational best practices

The *Geneva Manual* (both Chapter 1 on the implementation of the agreed UN GGE norms I and J, and Chapter 2 on the implementation of the agreed UN GGE norms F, G and H) compiles a number of good practices and practical approaches identified by non-state stakeholders that contribute to the protection of core Internet infrastructure and the resilience of critical services. These good practices are collected for each role, as identified as a result of multistakeholder regular consultations with the Geneva Dialogue experts (i.e. representatives of the private sector, civil society, academia and technical community).

Sources: Geneva Manual Chapter 1 available at: *https://genevadialogue.ch/wp-content/uploads/Geneva-Manual.pdf* and Geneva Manual Chapter 2 available at*: https://genevadialogue.ch/geneva-manual/chapter-2/*