kaspersky

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

Feedback by Kaspersky
June 2025

Kaspersky, a global cybersecurity company, welcomes the BPF's initiative to explore the importance of securing Internet access and protecting core Internet resources in contexts of conflict and crises. We recognize the BPF's vital role in addressing the most pressing issues in the global IT landscape and appreciate the opportunity to share our experiences and provide feedback on its questions.

General comments

We agree that there is a pressing need to clarify the roles and responsibilities of the multistakeholder Internet community – and the institutions within it – in securing core Internet resources and ensuring civilian access to the Internet during conflicts and crises. These roles and responsibilities could be defined through a set of tools, including clear policies and guidelines, stakeholder agreements, regular communication and coordination, established crisis response protocols, as well as capacity building and training.

In our view, key stakeholders should include governments, Internet service providers, network operators, the technical community (e.g., Internet Corporation for Assigned Names and Numbers, Internet Engineering Task Force), private sector companies, international organizations (e.g., ITU, UN), and NGOs.

1. **Do you agree with the way the problem is framed? Are there aspects that should be added, clarified, or reworded? How do you define the 'core Internet resources' referenced in the statement?**

We believe that the term 'core Internet resources' should be more clearly defined in order to establish a clear scope of discussion – including through the use of sector-specific examples. Although there is no universally adopted definition of 'core Internet resources' or 'critical information infrastructure', existing legislation and documents developed under the auspices of the United Nations can serve as useful references. For instance, the EU's *NIS2 Directive* (Annex I) or the *report* prepared by *the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (hereinafter referred to as 'UN GGE Report') may provide helpful guidance.

kaspersky

2. **What are the key challenges in ensuring the protection of the core Internet infrastructure and access during crises and conflicts?**

In addition to the need to clarify the roles and responsibilities of all stakeholders – as previously outlined by the BPF – the following challenges may also be highlighted:

- Maintaining network connectivity: Keeping Internet infrastructure operational despite physical damage or cyberattacks;
- Preventing DNS disruptions: Ensuring the continued functionality of the Domain Name System (DNS) to maintain stable and reliable online communication;
- Securing routing infrastructure: Protecting Border Gateway Protocol (BGP) and other routing systems from manipulation or attacks;
- Safeguarding critical infrastructure: Protecting key Internet infrastructure, such as undersea cables, data centers, and exchange points;
- Mitigating the impact of outages: Minimizing the effects of intentional or unintentional outages on core Internet infrastructure;
- Ensuring access to critical services: Maintaining access to essential online services, such as healthcare, finance, and emergency services;
- Coordinating incident response: Facilitating effective communication and collaboration among stakeholders to respond to crises and conflicts.

3. **Which existing norms, agreements, or processes are relevant to this issue? How effective are they in practice? Are there notable gaps?**

One could highlight, among others, the following documents, which could be relevant for the issue under consideration:

- *The UN GGE Report* includes, in particular, such provisions as "Do Not Damage Critical Infrastructure" (Norm 13(f)), "Protect Critical Infrastructure" (Norm 13 (g)), and "Respond to Requests for Assistance" (Norm 13(h));
- *Geneva Manual On Responsible Behaviour in Cyberspace (Chapter 2)* prepared by the Geneva Dialogue;
- *Hague (1899, 1907) and Geneva (1949) conventions* regulating the establishment of international legal standards for humanitarian treatment in war.

At the same time, the effectiveness of these documents is limited by one or more of the following factors:

- Lack of universal adoption, as not all countries or stakeholders participate in or adhere to these agreements;
- Insufficient enforcement mechanisms and limited consequences for non-compliance or violations;

- The evolving nature of conflicts, as new forms of conflict and cyber threats require updated norms and agreements.

4. **Can you share examples of successful practices or approaches—at a national, regional, or organisational level — that address these challenges?**

One initiative that could be highlighted in this context is the proposal by *the International Committee of the Red Cross (ICRC)* to create a 'digital red cross/crescent emblem' aimed at protecting essential medical infrastructure and the ICRC facilities in the digital realm. The record of this initiative – including obstacles it has faced – is particularly relevant, as healthcare sector is considered by the vast majority of experts as a part of critical information infrastructure.

Contact Person

For further information regarding this paper, please reach out to Jochen Michels, Head of Public Affairs, Europe, at jochen.michels@kaspersky.com.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.