PROTECTING CRITICAL INFRASTRUCTURES AGAINST SYSTEMIC HARMS

A path forward to overcome national discrepancies?

ISSUE BRIEF | NOVEMBER 2023

PARIS CALL
For trust and security in cyberspace

PARIS PEACE FORUM
de PARIS sur la PAIX

Over the past decade, increasingly robust and comprehensive regulatory frameworks, strategies and policy initiatives to protect critical infrastructures from cyber threats have been adopted at national and regional levels across the Globe[1]. Yet, recent years presented numerous examples of cyberattacks on sectors of vital importance to populations - widely documented by public authorities, the private sector and civil society[2]. Intergovernmental and multi-stakeholder cooperation in this respect has in the same period undeniably progressed, but remains limited by a lack of international harmonization.

Diverging national approaches[3] are especially a persistent obstacle to the adoption of a consensual definition of any critical infrastructure within the relevant international fora dealing with cyber policy. The final report of the United Nations Group of Governmental Experts (GGE) on Advancing responsible State behavior in cyberspace in the context of international security 2019/2021 suggest that critical infrastructures may refer to sectors “that provide essential services to the public”, or “that provide services across several States”, thus forming the “backbone of a society’s vital functions, services and activities”. However, it recalls explicitly that “each States determines which infrastructures or sector it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure"[4].

Two types of challenges have frequently been put forward against a universal definition, shared criteria or a common listing of critical infrastructures in the context of their protection against cyber threats. On the one hand, assessing criticality could only be done in-context, on the basis of ad hoc criteria pertaining to the interests, safety and security concerns as well as domestic capabilities of each State. On the other hand, a precise qualification at international level could prove counterproductive, making attacks on infrastructures outside the agreed scope more acceptable from a normative and political standpoint.

While these arguments do point to persistent difficulties, they should not encourage States not to seek better international convergence to secure vital services to populations from cyber harm. From an international security perspective, the ongoing fragmentation – and sometimes, divergence - of national strategies in qualifying critical infrastructures works against the effective implementation of agreed norms of responsible State behavior in cyberspace, including norms 13 (f), 13(g) and 13(h) of the 2015 GGE report[5], as well as other norms

[1] For a comparative study, see for instance: Jing de Jong-Chen, Bobby O’Brien, “A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China”, Digital Futures Project’s Paper, Wilson Center (2017)

[2] For an evidence-based quantitative analysis focusing on the healthcare sector, consult the CyberPeace Institute’s Cyber Incident Tracer

[3] For a study highlighting the divergent scopes of national definitions of critical infrastructure, see: OECD, “Reviews of Risk Management Policies, Good Governance for Critical Infrastructure Resilience”, OECD publication (2019), Chapter 3, Annex 3.B.

[4] United Nations General Assembly, Doc. A/76/135, 14 July 2021, pp. 12-13

[5] United Nations General Assembly, Doc A/70/174, 22 July 2015, pp. 7-8. These norms indicate that States should (i) refrain to conduct or support attacks again critical infrastructures located in a foreign jurisdiction; (ii) take appropriate measures to protect national critical infrastructures against ICT threats; (iii) consider international cooperation for critical infrastructures’ resilience when a malicious act occurs.

supported by the broader multi-stakeholder community such as Principles 1 and 2 of the Paris Call for Trust and Security in Cyberspace[6].

Starting from this premise and in light of the recent outcomes of multilateral cyber processes, the Paris Call community convened in a preparatory working group to explore what can be done to overcome political and methodological challenges so as to advance international cooperation for the protection and resilience of critical infrastructures against cyber harms.

Increasing transparency by States on their national strategy to their conceptualization of "critical infrastructures", and better information sharing on what they define as such domestically, including through common platforms, dedicated communication channels, standardized protocols and procedures might support convergence in a certain extent, in line with the GGE 2015 and 2021 reports' prescriptions and without contravening the sovereign right of States over their national infrastructures[7]. The question arises, however, whether additional cooperative efforts should be sought for infrastructures whose criticality has a fundamentally transnational dimension and whose disruption is likely to produce serious, cascading damages on a systemic scale. In such cases and building on numerous efforts to integrate cybersecurity and disaster risk reduction[8], an efficient protection against cyber threats might benefits from definitional harmonization which move away from particular national security interests and priorities - taking immediate harms to the population as the main reference point.

Reversing the approach could prove particularly relevant for those infrastructures that the GGE's 2021 reports describe as "providing services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet", that can be critical for some far-reaching activities such as "international trade, financial markets, global transport, communications, health or humanitarian action"[9]. A landmark normative work has been carried out in this respect by the Global Commission on the Stability of Cyberspace from 2017 to 2019, leading to a Call to Protect the Public Core of the Internet, defined as covering, without being limited to, "packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media"[10]. As with the other elements that fall under this definition, the integrity and availability of the infrastructures that make up the Public Core of the Internet should therefore be accorded

[6] Paris Call for Trust and Security in Cyberspace, Foundational Declaration, 2018. According to Principles 1 and 2, all relevant stakeholder commit to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures in order to Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure, as well as to prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.

[7] Andraz Kastelic, "International Cooperation to Mitigate Cyber Operations against Critical Infrastructure", United Nations Institute for Disarmament Research - UNIDIR (2021) , pp. 13-15

[8] In this regard, see : Abhilash Panda, Andrew Bower, "Bridging Cybersecurity and Disaster Risk Reduction", United Nations Office for Disaster Risk Reduction – UNDRR Working Paper (2020)

[9] United Nations General Assembly, Doc. A/76/135, 14 July 2021, p. 13

[10] Global Commission on the Stability of Cyberspace, "Definition of the Public Core, to Which the Norm Applies" (2018)

special protection against intentional and substantial damage resulting from the behavior of states and non-state actors[11].

Since then, the international cyber landscape has witnessed major shifts, fueled by the substantial increase of conflict in the physical world which in the same time provided key, fact-based findings on critical infrastructure protection. Recent technological developments, combined with a wider range of players and strategies in cyberspace, have also led to growing concern within the stakeholder community about a diversification of risks. International security concerns about the integrity of subsea communication cables[12]as well as the unveiling of cyber risks associated with the use of outer space by States and non-state actors[13] have for instance gained particular momentum since 2022, calls for further global efforts on protecting the Public Core of the Internet. To this end, the Paris Call's Working Group on Critical Infrastructure Identification has set three guiding priorities, that all interested stakeholders might consider in their own efforts:

1) Reassess whether the definition of the public core of the Internet in light of most recent geopolitical development and technology advancement while reviving discussions on the concept in international fora;

2) Systematize fact-finding and causality with regard to the damage and harm caused to populations by disruptions to the Public Core of the Internet;

3) Explore innovative, risk-based approach towards a protection scheme to ensure integrity and availability of Public Core of the Internet.

Such an effort should be undertaken in close connection with relevant international processes including within the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025 and as part of the negotiations on the future Cyber Programme of Action. Building on the achievements not only from States but also from the wider stakeholder community is indeed an important prerequisite, if only to discuss how to maintain relevance in light of recent shifts. The Paris Call's Working Group also benefits from the participation of key players in the field of cyber capacity-building, as this endeavor must especially tie in with cyber capacity-building's efforts on legal and policy design – in relation to relevant stakeholders in local and regional contexts. Lastly, the technical community should also be called upon to ensure the availability of reliable, cross-referenced data, at a time when there is still too little cross-fertilization with the policy community.

[11] Global Commission on the Stability of Cyberspace, "Call to Protect the Public Core of the Internet" (2017)
[12] For an international security perspective, see: Camino Kavanagh, "Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour", United Nations Institute for Disarmament Research – UNIDIR (2023)
[13] For a comprehensive analysis, see: Cybersecurity and Outer Space: A CIGI Essay Series, Centre for International Governance Innovation (2023)

PARIS CALL

For trust and security in cyberspace

About the Paris Call

The Paris Call for Trust and Security in Cyberspace, launched at the 2018 Paris Peace Forum, has become the reference multi-actor framework to advance common norms and principles for peace and security in cyberspace. Five years after its launch, it is now supported by more than 1200 actors, including 80 states, 700+ companies, and 380+ civil society organizations, rallied around nine common principles to defend a free, open and secure cyberspace through enhanced multistakeholder collaboration.

PARIS PEACE FORUM de PARIS sur la PAIX

About the Paris Peace Forum

In a world requiring more collective action, the Paris Peace Forum is a platform open to all seeking to develop coordination, rules, and capacities for concrete solutions to global problems where none exist. Year-round support activities and an annual event in November help better organize our planet by convening the world, boosting projects, and incubating initiatives.