GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

# STATEMENT ON THE INTERPRETATION OF THE NORM ON NON-INTERFERENCE WITH THE PUBLIC CORE

*22 September 2021*

The Global Commission on the Stability of Cyberspace (GCSC) welcomes the strong interest of the international community in its work, especially in the *norm on non-interference with the public core of the Internet*.[1] We are delighted that the concept of the public core of the Internet has been fully integrated in such diverse texts as the Paris Call for Trust and Security in Cyberspace and the Cyber Security Act of the European Union. We were also pleased to note that fundamental components of the public core norm, in particular the principles of our appeal to all actors to abstain from intentional activity that could substantially damage the general availability and integrity of the public core of the Internet, were endorsed in the 2021 reports of the UN Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE). The rising popularity of this norm shows that there is widespread interest in maintaining the current free, open, secure and interoperable Internet in the face of increasing malicious behavior directed against it. The fact that 18 of the 49 comments by states in response to the 2020 pre-draft of the OEWG directly or indirectly referenced the public core bears testimony to this common concern.

Recently, the work of the GCSC on the public core has been referenced in other documents as well, although the focus has been slightly different.[2] Some of these proposals may even cite or reference the GCSC definition of the public core and reproduce the norm in full, but ignore that, for reasons detailed in the GCSC final report, the Commission considers the multistakeholder model to be a cornerstone of cyberstability, as well as Internet governance. Fundamentally we believe that the norm of non-interference with the public core is an issue of governance "on" the Internet, and primarily a matter of moderating malicious state behavior, and not an issue of governance "of" the Internet, and therefore of Internet governance.

Firstly, the GCSC norm is primarily a norm of restraint, and largely orientated towards states. While our norm was clearly informed by the work of others[3], we also conducted an expert survey to help define the components of the public core, as well as the respective threats to it. It needs to be emphasized that, in the

[1] The GCSC norm on non-interference with the public core reads: "State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace." Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", November 2019.
[2] For instance, the contribution by the Russian Federation to the ITU CWG-Internet, "Risk Analysis of the Existing Internet Governance and Operational Model" (document CWG-Internet-16/4-E), 9 September 2021. It addresses (seemingly interchangeably) the "integrity and security", the "stability and integrity", and the "integrity, resilience, and stability" of the public core. The GCSC norm as well as the OEWG and GGE reports only refer to "availability and integrity" of the public core or Critical Information Infrastructure, respectively.
[3] In particular, the early work of the Association for Progressive Communication (Internet Rights Charter, 2006) and the later work of Dennis Broeders (The Public Core of the Internet, 2015).

vast majority of historic cases where the norm may be applied, the interference in question (whether intentional or not) was attributed to state-backed or state-affiliated organizations.[4] Only a single case was likely due to cybercrime.[5] Despite recent attempts to cast the main threat to the public core as resulting from cybercriminals,[6] it is in fact states and their affiliates whose activities pose the greatest risks. In recognition of this reality, both the OEWG and GGE reports echoed the GCSC in calling on states to abstain from activities that could interfere with the general availability and integrity of the Internet.[7]

Secondly, the GCSC norm implicitly and explicitly supports the current multistakeholder model of Internet governance as a means to ensure that cyberspace can be used safely and securely. As stated in our final report "Advancing Cyberstability", our commitment to the multistakeholder approach is one of practicality rather than innate philosophy. After all, "states acting alone or with only minimal non-state input cannot ensure the stability of cyberspace"[8]. This view is reflected throughout our work, including in the public core norm. The norm identifies four broad elements of the public core: (1) the packet routing and forwarding elements, (2) the naming and numbering systems, (3) the cryptographic mechanisms of security and identity, and (4) the physical transmission media.[9] In all but the physical transmission media, the key practical components of the current multistakeholder model are explicitly mentioned. For instance, in the naming and numbering systems (including the Domain Name System), the packet routing and forwarding elements (including the Border Gateway Protocol), as well as the cryptographic mechanisms of security and identity, the norm explicitly highlights the importance of protecting the current process of standardization and maintenance – which is commonly carried out by various non-state-led elements (such as the Intent Engineering Task Force and others) within the current multistakeholder model.

Most of the functionality elements of the public core are currently met by non-governmental actors, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and various Regional Internet Registries (RIRs). There is nothing in the GCSC norm to suggest that these key elements of the public core are not being well cared for by these actors. However, no extent of care is sufficient to address an unlimited reservoir of potentially malicious behavior. As described above, the only evidence of repeat behavior points to state-affiliated activity, and not cybercrime.

Further, the Tunis Agenda of 2005 provided an important distinction on the "use of" and the "development of" the Internet – and in the vast majority of cases the interference with the public core represents a "use of" problem, rather than one of "development" (including maintenance) of the Internet.[10] Thus, the logical approach to address this issue would be for all attempts of misuse and interference with the public core to be identified and condemned by all actors – in the international community of states, but also by the private sector and civil society.

---

[4] 'DNSpionage' (Nov. 2018), the Netnod attack (Dec. 2018 - Jan. 2019) forging a widely used software validation certificate, and DigiNotar (2011) in which certificate authorities were corrupted, provide examples of the potential disruptions that could generate widespread consequences for Internet users around the world.
[5] The DDoS attack on Dyn (2016). Due to lack of financial gains, it is even possible that this represents a case of "cyber vandalism".
[6] See for example ITU document CWG-Internet-16/4-E: "In the context of an aggravated international situation, Internet space uncontrolled militarization and cybercriminals significantly increasing their strength for attacking the global infrastructure, it is the states that must act as guarantors of the stability and integrity of the Internet's public core."
[7] Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, March 2021 (A/AC.290/2021/CRP.2) and Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, July 2021 (A/76/135).
[8] Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", November 2019.
[9] Global Commission on the Stability of Cyberspace, "Definition of the Public Core, to which the Norm Applies", May 2018.
[10] Article 32 of 2005 Tunis Agenda for an Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E. Article 55 also highlights the private-sector leadership of the development of the Internet.

Some actors may believe that "it is the states that must act as guarantors of the stability and integrity of the Internet's public core."[11] The GCSC does not believe this is correct. Instead, as it says in our final report:

> "Governments are, despite their unique responsibilities, not the exclusive protectors of this domain. Even if governments maintain a *de jure* monopoly over the legitimate use of force in cyberspace, they no longer have a practical monopoly on attacking and protecting this domain, nor can they prevent the proliferation and use of powerful cyber weapons. Rather, the technical community, civil society, and individuals also play a major role in the protection of cyberspace, including the promulgation of standards. Therefore, the multistakeholder approach is necessary to improve outcomes and ensure that the norms and policies supporting the stability of cyberspace are well-formed and avoid unwanted consequences."[12]

Concluding, the GCSC is encouraged by the growing recognition that the underpinnings of the global Internet are deserving of special consideration. We believe that this special consideration must reflect the unique heritage, identity and structure of the Internet as it currently functions. In the introduction to the recommendations of our report, it says "everyone is responsible for, and a multistakeholder approach is critical to, ensuring the stability of cyberspace,"[13] We stand by this view, and hope that both our report and our norm on non-interference with the public core can make a contribution towards this end.

[11] ITU document CWG-Internet-16/4-E
[12] Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", November 2019.
[13] Ibid.