GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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

CALL FOR CONTRIBUTIONS ON THE 2020 BPF ON CYBERSECURITY: SUBMISSION OF THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

October 2020

The Global Commission on the Stability of Cyberspace (GCSC) and its secretariat, The Hague Centre for Strategic Studies (HCSS), appreciates the opportunity to again contribute to the work of the Internet Governance Forum (IGF) Best Practice Forum Working Group. The Global Commission on the Stability of Cyberspace (GCSC) has long been an involved actor in previous IGF initiatives, and hopes that that it can continue to be an effective partner to the IGF in the future.

This year, upon the request of the IGF, the GCSC submits the following contribution to the call for contributions. This submission covers the primary contributions that the GCSC has made towards the development of norms in cyberspace, as well as some of the secondary norm-promotion actions taken by the HCSS via the Paris Call. We hope that this submission can be a valuable contribution to the final output of the IGF Best Practice Forum on Cybersecurity.

1. *Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at?*

The Global Commission on the Stability of Cyberspace and The Hague Centre for Strategic Studies (HCSS) is a signatory of the following agreements:

1.) The Global Commission on the Stability of Cyberspace (GCSC) norms
2.) The Paris Call for Security and Trust in Cyberspace

2. *What projects and programs have you implemented to support norms agreements your organization has agreed with?*

Norm development and advocacy lies at the core of the GCSC mandate. After the publication of its final report "Advancing Cyberstability" at the Paris Peace Forum in November 2019, the Commission and the Hague Centre for Strategic Studies (HCSS), the initiator and Secretariat of the GCSC, continued these efforts through:

(a) Norm Advocacy
(b) Communities of Interest
(c) Norm Monitoring

Taken together, these efforts lead to a better understanding of how the many cyber norms, CBMs, standards and principles relate to each other, and seeks out ways to advance norm advocacy, implementation, acceptance, and adherence across a wide range of stakeholders.

(a) Norm Advocacy

Presented below are just a few examples of the way in which the Commission's work on norms have been advocated and have already achieved success, either through honorable mention of the Commission's work or explicit affirmations of particular norms. While the COVID-19 pandemic has led to fewer advocacy possibilities, the GCSC looks to build on this further by advocating for norm acceptance and implementation various fora in order to enhance norm coherence across a wide range of stakeholders.

GCSC norms and final report translated into the six official UN languages

The GCSC Report "*Advancing Cyberstability*" has been translated and is now available in the official six languages of the United Nations: Arabic, Chinese, French, Russian, and Spanish. The GCSC Report "Advancing Cyberstability" has been prepared in English. In the event of any inconsistency or discrepancy between languages, the English version shall prevail.

EU Cybersecurity Act

The Norm to protect the public core of the Internet has been embedded into EU policy and law though its Cybersecurity Act, which also extends the mandate of ENISA to include the protection of the public core of the Internet.

The EU Cybersecurity Act represents a major step forward in EU cybersecurity policy. It aims to increase cybersecurity capabilities at EU level by establishing an EU-wide cybersecurity certification framework and promotes the current European Agency for Network and Information Security (ENISA) to a permanent EU Agency for Cybersecurity.

Paris Call for Trust and Security in Cyberspace

The Paris Call for Trust and Security in Cyberspace refers to five of the Commission's norms, making explicit reference to the Commission's flagship norm on protecting the public core of the Internet. Other norms referred to in the Call include preventing malign interference with electoral infrastructure, establishing a vulnerabilities equities process, ensuring basic cyber hygiene and prohibiting offensive cyber operations. It has already gained the backing of over 1000 official supporters, in which the GCSC is proud to be included.

United Nations

UN OEWG: When the GCSC was launched, it was the only multi-stakeholder initiative of its kind to bring in the expertise and voices from a wide range of stakeholders into the traditionally state-led multilateral discussions taking place in the United Nations. The Commission was the most cited non-state initiative at the discussions of the UN Open-Ended Working Group, which currently includes two of the GCSC norms – the norm to protect the public core of the Internet and the norm to protect electoral infrastructure in the pre-draft of its report.

UNSG: A Report of the UN Secretary-General A/74/62-E/2019/6 highlights the work of the Commission on norms of responsible behavior for reducing the risks to cyber stability. The report makes mention of the Commission in the section on 'building confidence and security in the use of information and communications technologies'. The report of the UN Secretary-General, entitled "Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels," is a response to the UN Economic and Social Council Resolution 2006/46.

In addition, the UN Secretary-General's High-level Panel on Digital Cooperation Report "The Age of Digital Interdependence" highlights the work of the Global Commission on the Stability of Cyberspace and its Singapore Norm Package.

IGF: The Commission always had strong presence at the IGF, where both German Chancellor Angela Merkel and 'Father of the Internet' Vint Cerf made a clear reference to the "need to protect the public core of the Internet". The GCSC has been a regular participant and session organizer of the IGF and contributor to its Best Practice Forum on Cybersecurity to advocate for its norms within the wider Internet governance community.

Cybersecurity Tech Accord

The Cybersecurity Tech Accord welcomed the GCSC Norm Package, and offered comments on enhancing stability in cyberspace during the GCSC request for consultation. The Tech Accord also released a statement to this effect, which can be read here. You can find the full Cybersecurity Tech Accord response to the GCSC consultation on its Singapore Norm Package here.

(b) Community of Interest

In its final report "Advacing Cyberstability", the GCSC recommends (recommendation 5) that State and non-state actors should establish and support Communities of Interest to advance the interpretation, adoption, and implementation of the cybersecurity norms put forward in its report and elsewhere, whether evidentiary standards for attribution are robust, and whether norms violators are being held accountable in a timely and effective manner.

The Hague Centre for Strategic Studies, as the GCSC Secretariat, has initiated a Community of Interest on protecting the public core of the Internet under the auspices of the Paris Call.

Public Core CoI: the Hague Centre for Strategic Studies will lead a community of interest on protecting the public core of the Internet

Responding to threats against the core protocols and services of the global Internet requires the cooperation of the full range of stakeholders. Most of the infrastructure, services, and products underpinning it are privately-owned, or governed and maintained by the civil society functioning as a technical community.

Whilst the idea of protecting the core Internet functions has a longer history, the notion only recently became the subject of various norm proposals, most notably by the Global Commission on the Stability of Cyberspace (GCSC), which was initiated by the The Hague Centre for Strategic Studies (HCSS). Building on the GCSC Report "Advancing Cyberstability" which calls for the adoption of specific "Communities of Interest", HCSS will lead a "Community of Interest on Protecting the Public Core of the Internet" (Public Core CoI). This concerted multistakeholder initiative will gather committed supporters for the general principle of protecting the public core in a regular working group.

This group will likely examine the need to further refine the concept, discuss propagation, and explore options for implementation and monitoring of the principle as well as related norms. It will convene key stakeholders to raise awareness of the threats against the core Internet protocols and functions, develop best practices and policy proposals for adoption and implementation, and advance common understandings of violations of the principle.

Organizations interested in joining the Public Core CoI can write to cyber@hcss.nl.

(c) Norm Monitoring

The HCSS has also been acutely monitoring the uptake of its norms since the GCSC's inception. Two of the norms that the GCSC is most associated with are its first two: the norm of non-interference in the public core of the internet and the norm to protect electoral infrastructure. Both of these norms are increasingly receiving widespread support from governments, For instance, as part of the Public Core COI, HCSS is especially interested in the adoption of a norm advocating for the protection of the public core of the internet, and maintains an active dataset of states which endorse this norm. At present, through analyzing statements made at the OEWG and signatories to the Paris Call, the HCSS can conclude that there is an ever-growing number of supporters for this norm.

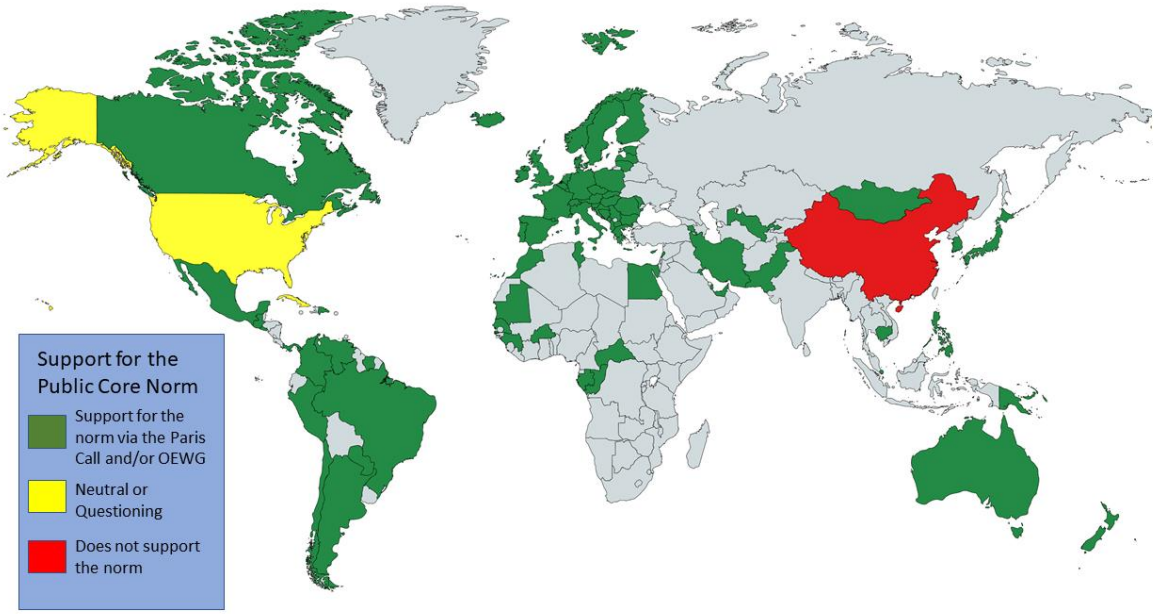

Figure 1: State Support for the Public Core Norm through the Paris Call for Trust and Security in Cyberspace and the submissions to the UN Open-Ended Working Group.

HCSS is also developing a Cyber Norms Observatory (CNO) of over 900 norms, principles, CBMs, and technical standards from all stakeholders, using text-mining and data visualization tools to visualize policy clusters and identify possible synergies and gaps. The CNO aims to map the cyberspace regime complex and the norms, principles, confidence building measures (CBMs) and standards that inhabit it. The tool visualizes this as a social network through which the user can identify policy and stakeholders clusters, as well as norm relations, including norm coherence, comparison, conflict, and acceptance. This allows for a schematic and easily performed stakeholder analysis and accompanying drilldown on the specific interests of each stakeholder. To this end, the CNO makes use of a combination of analytical methods, including social network analysis, text mining, and machine learning. It empowers policy makers to make more intelligent decisions by combining strong content knowledge with quantitative data analytics.

3. *Are you aware of any other cybersecurity agreements that describe specific norms in cyberspace? If so, could you provide the following information?*

The Paris Call for Trust and Security in Cyberspace.

4. *Are there cybersecurity issues you believe should be addressed by a cybersecurity agreement which are currently not?*

Currently, the IGF BPF background document only includes the six norms of the GCSC Singapore Norms Package, which does not include the first two GCSC norms on the protection of the public core and electoral infrastructure. For a full list of the GCSC norms, please see https://cyberstability.org/norms/:

The Eight Norms of the GCSC

1. NON-INTERFERENCE WITH THE PUBLIC CORE
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.

2. PROTECTING ELECTORAL INFRASTRUCTURE
State and non-state actors must not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

3. NORM TO AVOID TAMPERING
State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

4. NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS
State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.

5. NORM FOR STATES TO CREATE A VULNERABILITY EQUITIES PROCESS
States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.

6. NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES
Developers and producers of products and services on which the stability of cyberspace depends should (1) prioritize security and stability, (2) take reasonable steps to ensure that their products or services are free from significant vulnerabilities, and (3) take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.

7. NORM ON BASIC CYBER HYGIENE AS FOUNDATIONAL DEFENSE
States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

8. NORM AGAINST OFFENSIVE CYBER OPERATIONS BY NON-STATE ACTORS
Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

Furthermore, the COVID-19 epidemic has led to a dramatic increase in the amount of cyberattacks taking place against public infrastructure, most notably hospitals and the wider healthcare sector.[1] We support the condemnation of these kind of attacks and support the International Committee of the Red Cross that has issued a call to protect medical services and medical facilities against cyberattacks of any kind.

[1] Michael Chertoff, Latha Reddy and Alexander Klimburg, "Facing the Cyber Pandemic," *Project Syndicate* June 11, 2020. https://www.project-syndicate.org/commentary/pandemic-cybercrime-demands-new-public-core-norm-by-michael-chertoff-et-al-2020-06?barrier=accesspaylog