GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

ADVANCING CYBERSTABILITY

FINAL REPORT FACT SHEET
NOVEMBER 2019

On 12 November 2019, the Global Commission on the Stability of Cyberspace (GCSC) issued its final report: ***Advancing Cyberstability***, at the 2019 Paris Peace Forum. The report fulfills the multistakeholder Commission's three-year mission to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace. The report proposes a framework that will advance cyberstability, a set of four principles, six recommendations, and eight norms that address critical elements of implementation, monitoring, and accountability.

GCSC Cyberstability Framework

The overarching framework is designed to assist the international community in promoting the stability of cyberspace while taking into consideration the rapid, unprecedented pace of technological change that significantly and continuously alters cyberspace.

The GCSC's proposed Cyberstability Framework features seven core areas:

1. Multistakeholder engagement
2. Cyberstability principles
3. Development and implementation of voluntary norms
4. Adherence to international law
5. Confidence building measures
6. Capacity building
7. Open promulgation and widespread use of technical standards

GCSC Principles & Norms

The Commission identifies four principles that can be considered critical to cyberstability and help pave the way for norms of responsible behavior:

- **Responsibility:** Everyone is responsible for ensuring the stability of cyberspace.
- **Restraint:** No state or non-state actor should take actions that impair the stability of cyberspace.
- **Requirement to Act:** State or non-state actors should take reasonable and appropriate steps to ensure the stability of cyberspace.
- **Respect for Human Rights:** Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

Building on these principles, the Commission crafted eight norms:

1. 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. 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. 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. State and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes.
5. 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. 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. States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.
8. Non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur.

GCSC Report Recommendations

The Commission concluded its report with six recommendations that underline the need for strengthening the multistakeholder model, promoting norms adoption and their implementation, and ensuring that those who violate norms are held accountable. Each of the recommendations stem from the defined principles, offering what measures should be adopted, and suggesting how they might be achieved to ensure the stability of cyberspace.

Specifically, the Commission recommends that:

1. State and non-state actors adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action.
2. State and non-state actors, consistent with their responsibilities and limitations, respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.
3. State and non-state actors, including international institutions, increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of different parties.
4. State and non-state actors collect, share, review, and publish information on norms violations and the impact of such activities.
5. State and non-state actors establish and support Communities of Interest to help ensure the stability of cyberspace.
6. A standing multistakeholder engagement mechanism be established to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.

For a copy of the GCSC report, please click on ***Advancing Cyberstability***.

About the Commission

Launched at the 2017 Munich Security Conference, the mission of the Global Commission on the Stability of Cyberspace is to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace. The Commission helps to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity, in particular by finding ways to link the dialogues on international security with the new communities created by cyberspace. For more information about the Commission, please visit **www.cyberstability.org**.

For more information, please contact: **Louk Faesen** (loukfaesen@hcss.nl) or **Anneleen Roggeman** (aroggeman@eastwest.ngo).