BACKGROUND

Conflict between states will take new forms, and cyber-activities are likely to play a leading role. The rise of offensive cyber operations risks undermining the peaceful use of cyberspace to facilitate economic growth and the expansion of individual freedoms. Cyberspace is becoming an increasingly exploited resource that few feel compelled to take responsibility for, leading to a steady decay of the stability and security of the entire environment itself. To counter these developments more dialogue, research, and actionable initiatives are needed.

Cyberspace is formed and governed by a range of different institutions and processes. A major challenge is insufficient awareness and mutual acceptance among the various cyberspace communities working on issues related to international security in and of cyberspace. By finding ways to link the international security and Internet communities, the Commission has a genuine opportunity to contribute to an essential task: supporting policy coherence related to the security and stability in and of cyberspace.

DELIVERABLES

1. Facilitating information exchange:
From 2017-2020, the Commission will meet physically four times per year, encouraging the flow of information and knowledge across various cyberspace initiatives. An active outreach program encourages cross-fertilization and capacity building amongst initiatives.

2. Supporting basic research:
Together with the Research Advisory Group, the Commission funds and conducts research on norms as well as on emerging themes and ideas of relevance to the stability of cyberspace.

3. Advocating proposals for action:
The Commission formulates recommendations for action, applicable to both state and non-state led initiatives. These include Commission Positions and White Papers. The Commission will advocate for these recommendations in capitals, corporate headquarters, and civil society centers, as well as the wider public.

SET-UP

CIVIL SOCIETY
INDUSTRY
GOVERNMENTS

3 CHAIRS & 26 COMMISSIONERS

SECRETARIAT
RESEARCH ADVISORY GROUP
MANAGEMENT BOARD
GOVERNMENT ADVISORY BOARD
THE RULES OF THE ROAD

GCSC PROPOSED NORMS OF BEHAVIOR IN CYBERSPACE

In international security, norms\(^1\) have become a common standard for agreeing on what constitutes acceptable action in cyberspace, accompanying and expanding on existing legal understanding rather than attempting to craft new law. Often these norms are described as the “rules of the road” that determine acceptable and proscribed behavior.

The Commission does not begin its work in a vacuum. Its efforts are informed in particular by the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE) report of 2013 and 2015 that proposed 11 crucial norms. It has also been inspired by developments in the G20, the G7, regional organizations, as well as non-state norms developed by Microsoft, and ISOC, to name but a few. It has also greatly benefited from the work done within Internet governance, including the work of NETmundial and the Internet Governance Forum.

Norms are foundational for better governance, and therefore the initial focus of the Commission’s work. They form a test of “what needs to be done” – a practical sense test of what practical and operational steps need to be undertaken to achieve some measure of “cyber stability”.

Throughout its deliberations, the GCSC is guided by significant shared core beliefs. These include the importance of a democratic, multi-stakeholder approach to governance, the necessity to promote development and growth, the need to balance rights and responsibilities for both state and non-state actors, and the centrality of cyberspace remaining open and unimpeded in its operations. The GCSC aims to expand the global understanding of responsible behavior in cyberspace for both states and non-state actors.

NORM TO PROTECT THE PUBLIC CORE OF THE INTERNET

Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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.\(^2\)

NORM TO PROTECT THE ELECTORAL INFRASTRUCTURE

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

\(^{1}\) Norms are voluntary, legally non-binding commitments. Over time they can crystallize into international law. Norms prescribe a positive or a negative obligation. The overall stability of the cyberspace is also served through capacity and confidence building efforts.

\(^{2}\) Elements of the public core include, inter alia, Internet routing, the domain name system, certificates and trust, and communications cables, which have been further defined in the Definition of the Public Core, to which the norm applies.
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.

NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS

State and non-state actors should not commandeer others’ ICT resources for use as botnets or for similar purposes.

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.

NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES

Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, 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.

NORM ON BASIC CYBER HYGIENE AS FOUNDATION DEFENSE

States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.

NORM AGAINST OFFENSIVE CYBER OPERATIONS BY NON-STATE ACTORS

Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur.
CHAIRS
Marina Kaljurand Estonia
Michael Chertoff USA
Latha Reddy India

COMMISSIONERS
Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brazil
Isaac Ben-Israel Israel
Scott Charney USA
Frédérick Douzet France
Anriette Esterhuysen South Africa
Jane Holl Lute USA
Nigel Inkster UK
Khoo Boon Hui Singapore
Wolfgang Kleinwächter Germany
Olaf Kolkman Netherlands
Lee Xiaodong China
James Lewis USA
Jeff Moss USA
Elina Noor Malaysia
Joseph S. Nye, Jr. USA
Christopher Painter USA
Uri Rosenthal Netherlands
Ilya Sachkov Russia

Samir Saran India
Marietje Schaake Netherlands
Motohiro Tsuchiya Japan
Bill Woodcock USA
Zhang Li China
Jonathan Zittrain USA

SPECIAL REPRESENTATIVES AND ADVISORS
Carl Bildt Sweden
Vint Cerf USA
Sorin Ducaru Romania
Martha Finnemore USA

DIRECTORS
Alexander Klimburg Austria
Bruce W. McConnell USA

RESEARCH ADVISORY GROUP CHAIRS
Sean Kanuck USA
Koichiro Komiyama Japan
Marilia Maciel Brazil
Liis Vihul Estonia
Hugo Zylberberg France

SECRETARIAT

PARTNERS

SPONSORS
Ministry of Foreign Affairs of Estonia
GLOBSEC

SUPPORTERS
Black Hat USA
Packet Clearing House
Tel Aviv University

GCSC