GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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

OUR MISSION

THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE (GCSC) ENGAGES THE FULL RANGE OF STAKEHOLDERS TO DEVELOP PROPOSALS FOR NORMS AND POLICIES TO ENHANCE INTERNATIONAL SECURITY AND STABILITY, AND GUIDE RESPONSIBLE STATE AND NON- STATE BEHAVIOR IN CYBERSPACE.

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.**

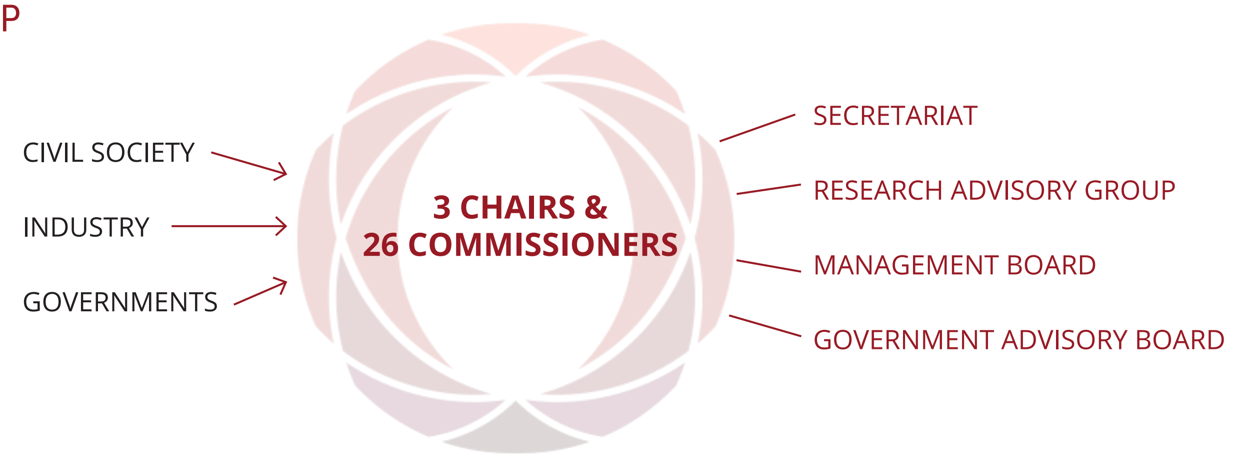
DELIVERABLES

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

CALL TO PROTECT THE PUBLIC CORE OF THE INTERNET

New Delhi, November 2017

The Internet has changed the world, fueling political, economic, and social growth. More generally, cyberspace promotes communication, commerce, education, human rights and livelihood on every level. To continue this progress, we believe that the stability of cyberspace is essential for the good of humanity now and into the future.

As with all critical infrastructures, the technology that underpins the global Internet is imperfect. Technology can break, and the existence of flaws, vulnerabilities, malicious actors and the development of offensive capabilities create conditions of instability that put the benefits of cyberspace in jeopardy.

The Global Commission on the Stability of Cyberspace was established to enhance international peace, security, and stability by proposing norms and initiatives to guide responsible state and non-state behavior in cyberspace. A commitment to norms, together with the application of international law, can significantly enhance cyber stability.[1]

As a first step, recognizing the global reliance on cyberspace, the increasing dependence of other infrastructures on its reliability, and the potentially dramatic consequences of its disruption, the Commission urges all stakeholders to adhere to the following norm that sustains the general availability and integrity of the Internet.

NON-INTERFERENCE WITH THE PUBLIC CORE

> **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]

[1] Norms are voluntary, 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***.

CALL TO PROTECT THE ELECTORAL INFRASTRUCTURE

Bratislava, May 2018

PROTECTING 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.**

BACKGROUND

Of all the rules, precepts and principles that guide the conduct of states in the comity of nations, the norm of non-interference is perhaps held most sacred. Article 2(4) of the United Nations Charter articulates this norm and elevates it as a principle of legal, and thus, binding character:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

Through this provision, the framers of the Charter acknowledged that the gravest threats to the principle of non-intervention came from coercive measures directed at a state's physical or political autonomy, as, indeed, both are essential to state sovereignty. The territory controlled by a state may be a manifestation of its sovereign capacity, but it is worthless without the enjoyment of political agency and independence. Moreover, nothing reflects genuine political independence more than national participatory processes, such as elections, conducted freely and fairly. The UN Charter sought to grant strong protections against undue external interference. Those protective measures have now come to be challenged again in the digital age.

The advent of the Internet and the accompanying wave of "digitalisation" has opened up new opportunities for the material, cultural and intellectual advancement of communities across the world. But it has also pried open the possibility of malicious actors—acting alone, collectively, or on behalf of states— manipulating elections through digital means. With national participatory processes becoming more complex in scale and sophistication, there has been a burgeoning of data, institutions and infrastructure to manage them. Many countries today publish their electoral rolls—a basic, traditional guarantee against voting manipulation or fraud—online, exposing such databases to cyber attacks and exploitation. Similarly, electoral voting instruments are used in far flung and remote areas of a country, where its operators are not fully abreast of the risks and concerns associated with their digital manipulation. Voting software suppliers and computer systems at the local or "booth" levels remain susceptible to such intrusions as well.

Seized of the growing number and intensity of threats to participative processes, the Global Commission on the Stability of Cyberspace recommends stronger national measures and effective international cooperation to prevent, mitigate and respond to cyber intrusions against the technical electoral infrastructure. The Commission acknowledges that the actual conduct of elections or participatory processes at the regional, local or federal level is firmly the remit of states, to be carried out in accordance with their respective national laws. Nevertheless, the cyber attacks on their electoral infrastructure may originate from outside the borders, necessitating multilateral cooperation resolution. As more countries opt to digitise their election machinery, the risks and vulnerabilities associated with such infrastructure increase manifold, as does the prospect of a major, offensive cyber operation. A modest first step to effective multilateral cooperation would be a pledge or commitment from governments to refrain from engaging in cyber operations against the technical electoral infrastructure of another state. In recommending this norm, the Commission merely affirms the numerous international legal protections already afforded against external interference in the internal affairs of another state.

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

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Microsoft

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

SPONSORS

Ministry of Foreign Affairs of Estonia
GLOBSEC

SUPPORTERS

Black Hat USA
Packet Clearing House

GCSC