GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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

CALL TO PROTECT THE ELECTORAL INFRASTRUCTURE

Bratislava, May 2018

PROTECTING ELECTORAL INFRASTRUCTURE[1]

> **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.

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.

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