

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE
TO PROMOTE PEACE AND PROSPERITY

MEETING WITH ICANN GOVERNMENTAL ADVISORY COMMITTEE

27 JUNE 2019 | ICANN65, MARRAKESH

GCSC

MISSION STATEMENT



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

“To engage 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.”

TIMELINE FULL COMMISSION MEETINGS



02/17	05/17	11/18	05/18	09/18	01/19	03/19	10/19	11/19
Launch Munich Security Conference	Tallinn	Delhi	Bratislava	Singapore	Geneva	Kobe	Addis Ababa	GCSC report

GCSC MEMBERSHIP



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

CHAIRS

Michael Chertoff USA
Latha Reddy India

COMMISSIONERS

Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brazil
Isaac Ben-Israel Israel
Scott Charney USA
Frédéric Douzet France
Anriette Esterhuysen South Africa
Jane Holl Lute USA
Nigel Inkster UK
Khoo Boon Hui Singapore
Marina Kaljurand Estonia
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 ADVISORS

Carl Bildt Sweden
Vint Cerf USA
Sorin Ducaru Romania
Martha Finnemore USA

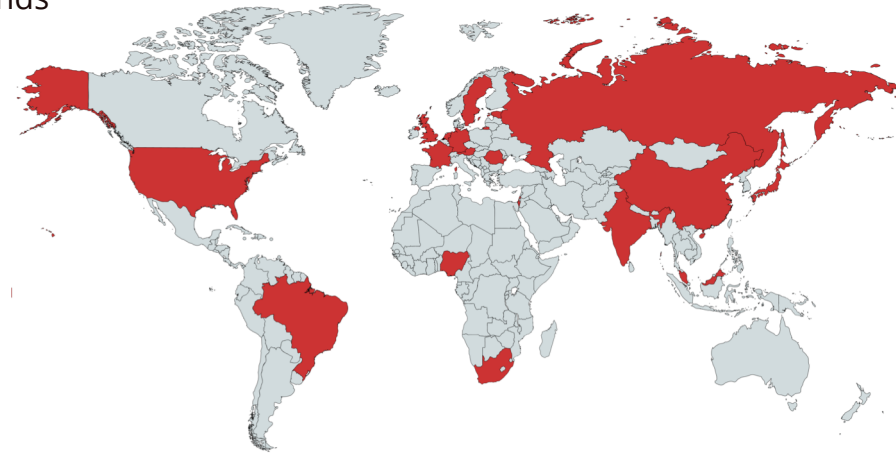
DIRECTORS

Alexander Klimburg Austria
Bruce W. McConnell USA

RESEARCH ADVISORY

GROUP CHAIRS

Sean Kanuck USA
Koichiro Komiyama Japan
Marilia Maciel Brazil
Liis Vihul Estonia



SECRETARIAT



SPONSORS

Japanese Ministry of Internal Affairs and Communications
GLOBSEC
UNIDIR
Federal Department of Foreign Affairs of Switzerland
Ministry of Foreign Affairs of Estonia

SUPPORTERS

Black Hat USA
Google
DEF CON
Packet Clearing House
Tel Aviv University
European Union Delegation to the UN in Geneva
Municipality of The Hague

PARTNERS



Ministry of Foreign Affairs

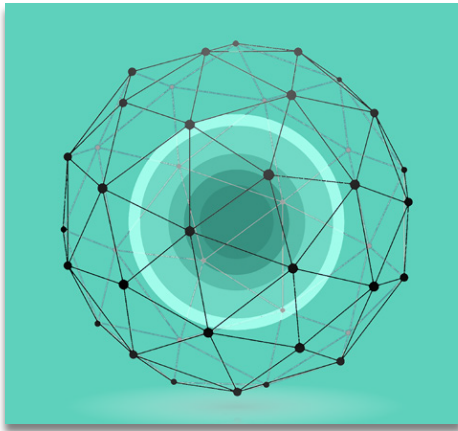


MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

CALL TO PROTECT THE PUBLIC CORE OF THE INTERNET



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



“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.”



ELEMENTS OF THE PUBLIC CORE OF THE INTERNET

1. Packet routing and forwarding
2. Naming and numbering systems
3. The cryptographic mechanisms of security and identity
4. Physical transmission media

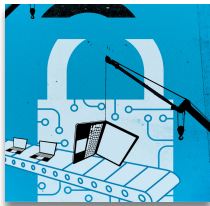
GCSC NORMS



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



NORM TO
PROTECT THE
PUBLIC CORE OF
THE INTERNET



NORM TO AVOID
TAMPERING



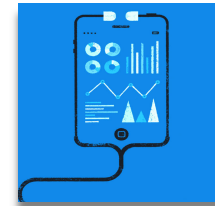
NORM FOR
STATES TO
CREATE A VEP



NORM AGAINST
COMMANDEERI
NG OF ICT
DEVICES INTO
BOTNETS



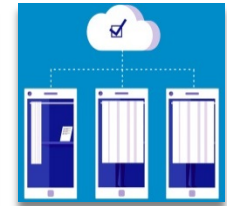
NORM TO
REDUCE AND
MITIGATE
SIGNIFICANT
VULNERABILITIES



NORM ON BASIC
CYBER HYGIENE
AS
FOUNDATIONAL
DEFENSE



NORM AGAINST
OFFENSIVE
CYBER
OPERATIONS
BY NON-STATE
ACTORS



NORM TO
PROTECT THE
ELECTORAL
INFRASTRUCTURE



GCSC

NORM ENDORSEMENTS



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



547 like-minded states, companies and civil society organizations endorse 5 out of 8 GCSC norms, and made special reference to the public core of the Internet

Norm to protect the public core of the Internet part of ENISA's mandate through the EU Cybersecurity Act

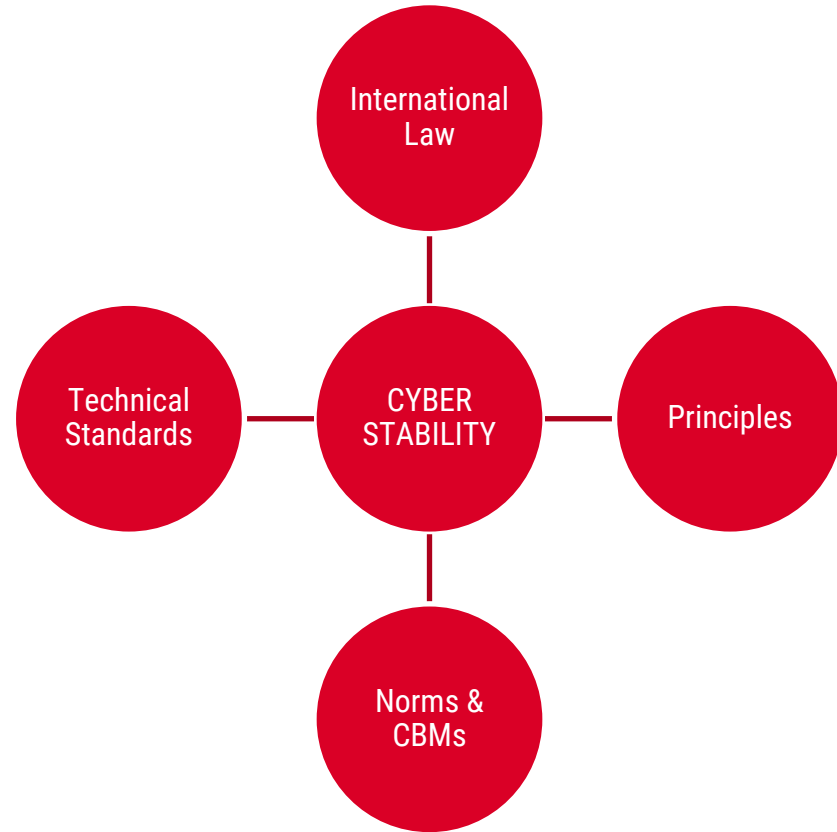
The Tech Accord welcomes the GCSC norms, and made special reference to the norm to avoid tampering, norm against commandeering of ICT devices into botnets, and the norm for states to create a VEP

CYBER STABILITY

WORKING DEFINITION

Stability of cyberspace is the condition where individuals and institutions can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services in cyberspace is generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.

Stability is based on adherence to existing international law (including international human rights law), common understandings of acceptable behavior, transparency, confidence-building measures facilitated through capacity-building, and by the open promulgation and widespread use of technical standards that ensure cyberspace is resilient.





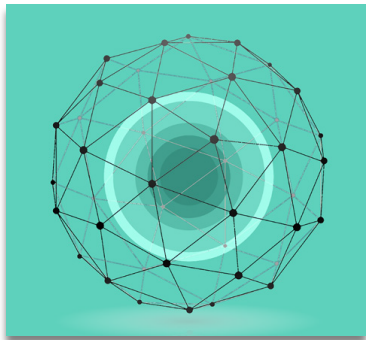
GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org
[@theGCSC](https://twitter.com/theGCSC)
info@cyberstability.org
cyber@hcss.nl

GCSC NORMS

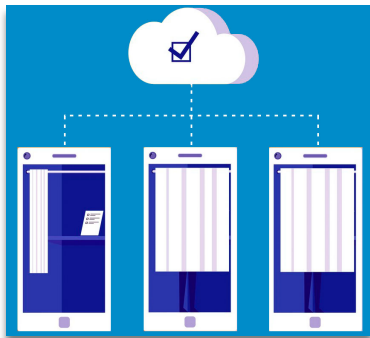


GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



CALL 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.”



CALL 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.”

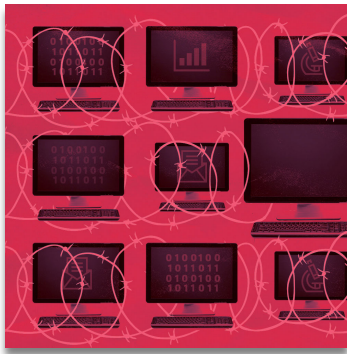


GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



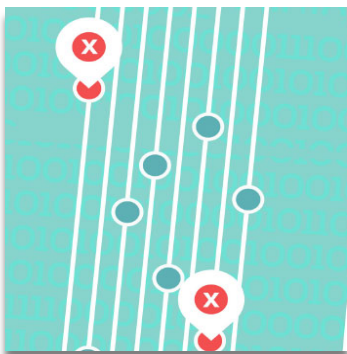
NORM TO AVOID TAMPERING

“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 FOUNDATIONAL 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.”

UN GGE 2015 REPORT



GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

“While states have a primary responsibility to maintain a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.”