
GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE
ICANN64 KOBE, JAPAN

GCSC
MEMBERSHIP

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre for Strategic Studies

EastWest INSTITUTE

Ministry of Foreign Affairs

CSR SINGAPORE

Microsoft

Afilias

Internet Society

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

GCSC

MISSION STATEMENT

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

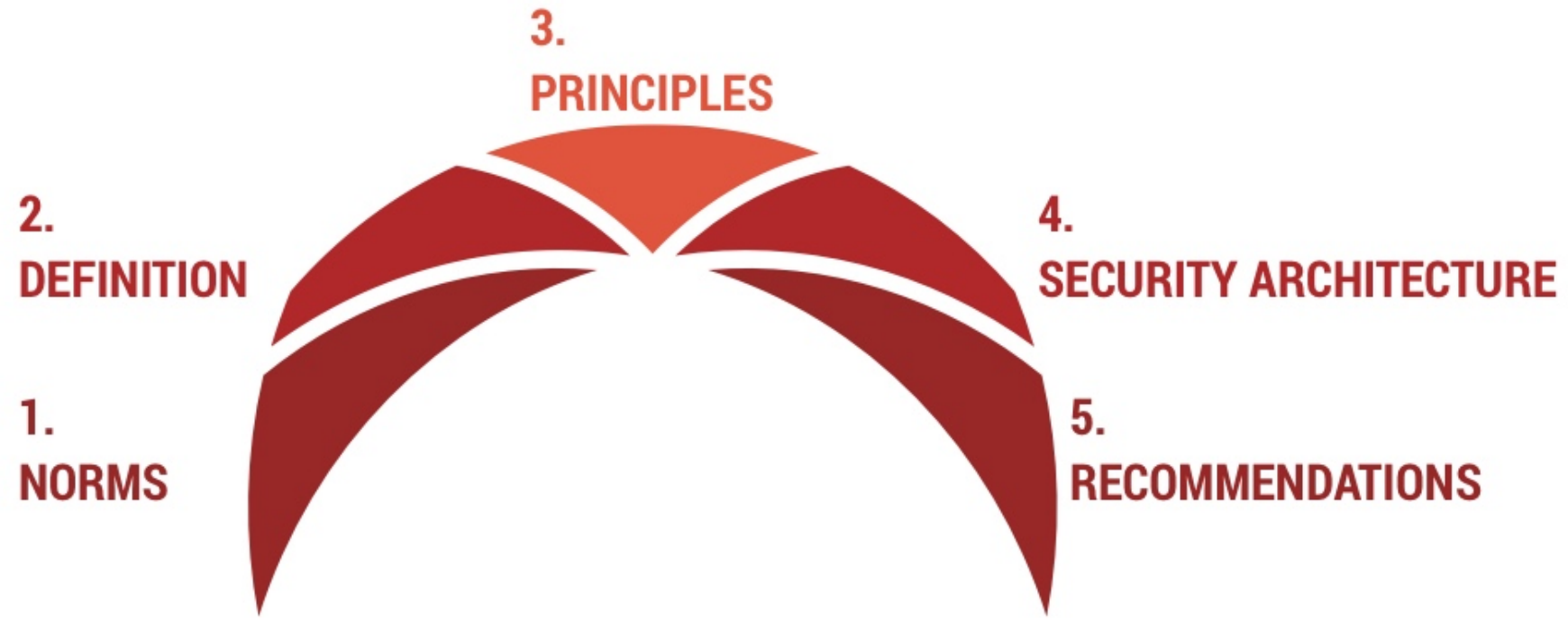
"To engage the full range of stakeholders to develop **proposals for norms and policies** to enhance international security and stability, and guide responsible state and non-state behavior in cyberspace."

TIMELINE FULL COMMISSION MEETINGS

02/17	05/17	11/18	05/18	09/18	01/19	03/19	(additional meetings)	(12/19 Final report)
Launch Munich Security Conference	Tallinn	Delhi	Bratislava	Singapore	Geneva	Kobe		

GCSC
METHOD

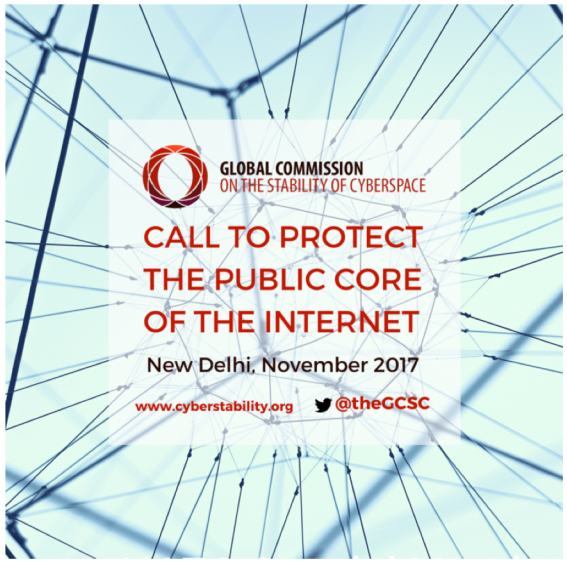
GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



GCSC
METHODOLOGY NORMS

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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."

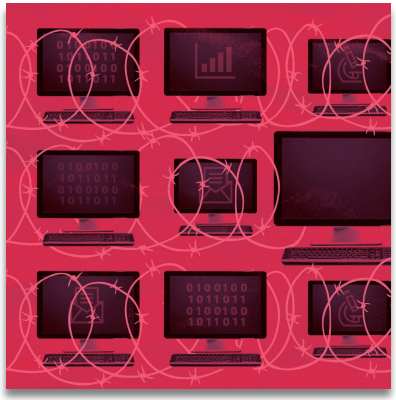
CALL TO PROTECT
THE ELECTORAL INFRASTRUCTURE

"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."

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.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

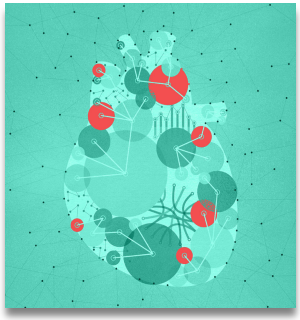


NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS

"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

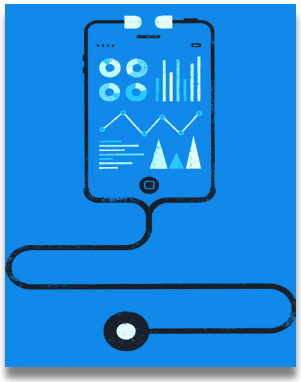
"States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure."



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."

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE



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."

CYBER STABILITY
WORKING DEFINITION

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

Stability in cyberspace is the condition where state and non-state actors are confident in their ability to use cyberspace safely and securely, and where the availability and integrity of services in cyberspace is generally assured.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

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