



# **GCSC, UN GGE AND UN OEWG NORMS PROCESS, FRAMEWORKS AND CONFIDENCE BUILDING MEASURERS (CBM)**

@ the

**AFRICA ICT ALLIANCE (@AfICTA)**

by:

**Consultancy Support Services (CS2) Ltd.,**



**[info@consultancyss.com](mailto:info@consultancyss.com)**

The Pavilion, International Conference Center, Abuja

29 November 2019

Consultancy Support Services (CS2) Limited, [info@consultancyss.com](mailto:info@consultancyss.com)

# Its 4 People, by People & about People



## Cyberstability

- Availability
- Integrity
- Requires - shared vision: Disagreements and changes which affect cyberspace must be managed in relative peace
- State & Non-state actors should be guided by similar principles and bound by similar norms

**Cyberspace is designed, deployed, and operated primarily by non-state actors**

## Economies need stability – integrity & trust

- Security starts with you and I
- Nation and its citizens must understand the rules of the game – education
- Take responsibility for our own destiny and not be overly dependent on other economies for our wellbeing or guidance.
- We must act in our own enlightened national best interests
- Remain eternally vigilant.

**A principle of right action  
binding upon the members  
of a group and serving to  
guide, control, or regulate  
proper and acceptable  
behavior**



## Responsibility - multistakeholder

**Restraint** – Aligns with United Nations (UN) UN General Assembly (**UNGA**):

- a. UN High-Level Panel on Digital Cooperation (**HLP**)
- b. UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (**GGE**),
- c. UN Open-Ended Working Group (**OEWG**)`

## Requirement to Act

## Respect for Human Rights

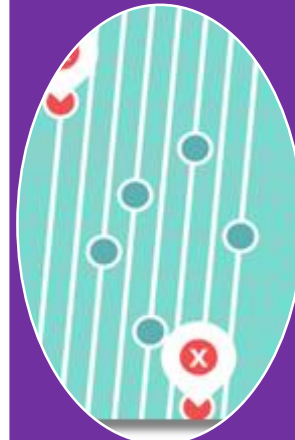
# SCOPE OF GCSC NORMS



***“Public Commons”***  
**Norm to Protect the Public Core**



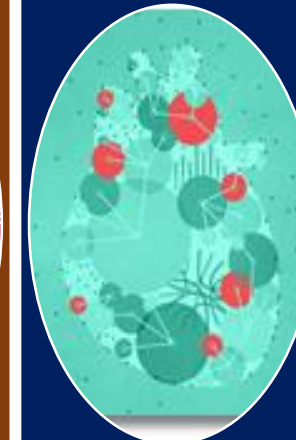
***“Don’t intentionally create flaws”***  
**Norm to Avoid Tampering**



***“Disclose & fix flaws”***  
**Norm for States to Create a Vulnerability Equities Process**



***“Conscription”***  
**Norm Against Commandeering of ICT Devices into Botnets**



***“Due Diligence”***  
**Norm to Reduce and Mitigate Significant Vulnerabilities**



***“End Users Keep it Clean”***  
**Norm on Basic Cyber Hygiene as Foundational Defense**



***“No hack back”***  
**Norm Against Offensive Cyber Operations by Non-State Actors**



***“non-intervention in national participatory processes”***  
**Norm to Protect the Electoral Infrastructure**

Critical **OF** Cyberspace

**Cyberspace Stability**

Critical **IN** 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."

## \* Elements of the Public Core of the Internet

- Packet routing and forwarding
- Naming and numbering systems
- The cryptographic mechanisms of security and identity
- Physical transmission media

**Not Content like Fake News or Hate Speech**

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."



### 3. 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.”

### 4. 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.”

### 5. 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.”

### 6. NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES

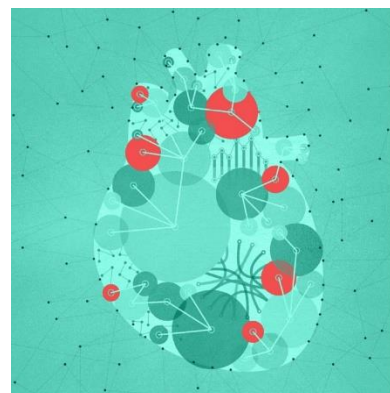
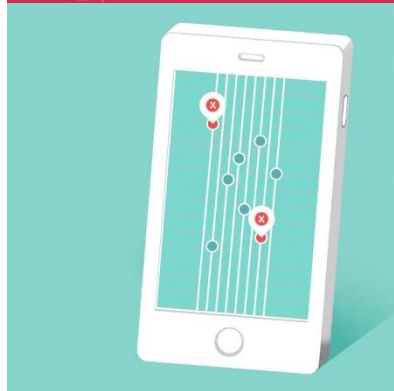
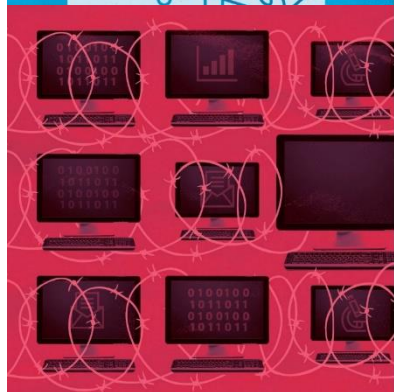
“Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are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

### 7. NORM ON BASIC CYBER HYGIENE AS FOUNDATIONAL DEFENSE

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

### 8. 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.”





**“Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace **safely and securely, where the availability and integrity of services and information** provided in and through cyberspace are generally assured, where **change is managed in relative peace,** and where tensions are resolved in a non-escalatory manner.**

**State and non-state actors must adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action.**

**State and non-state actors, consistent with their responsibilities and limitations, must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences.**

**State and non-state actors, including international institutions, should increase efforts to train staff, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of different parties.**

**State and non-state actors should collect, share, review, and publish information on norms violations and the impact of such activities.**

**State and non-state actors should establish and support Communities of Interest to help ensure the stability of cyberspace.**

**The GCSC recommends establishing a standing multistakeholder engagement mechanism to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.**



**74 states, 25 Public Authorities, 609 companies and 333 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**

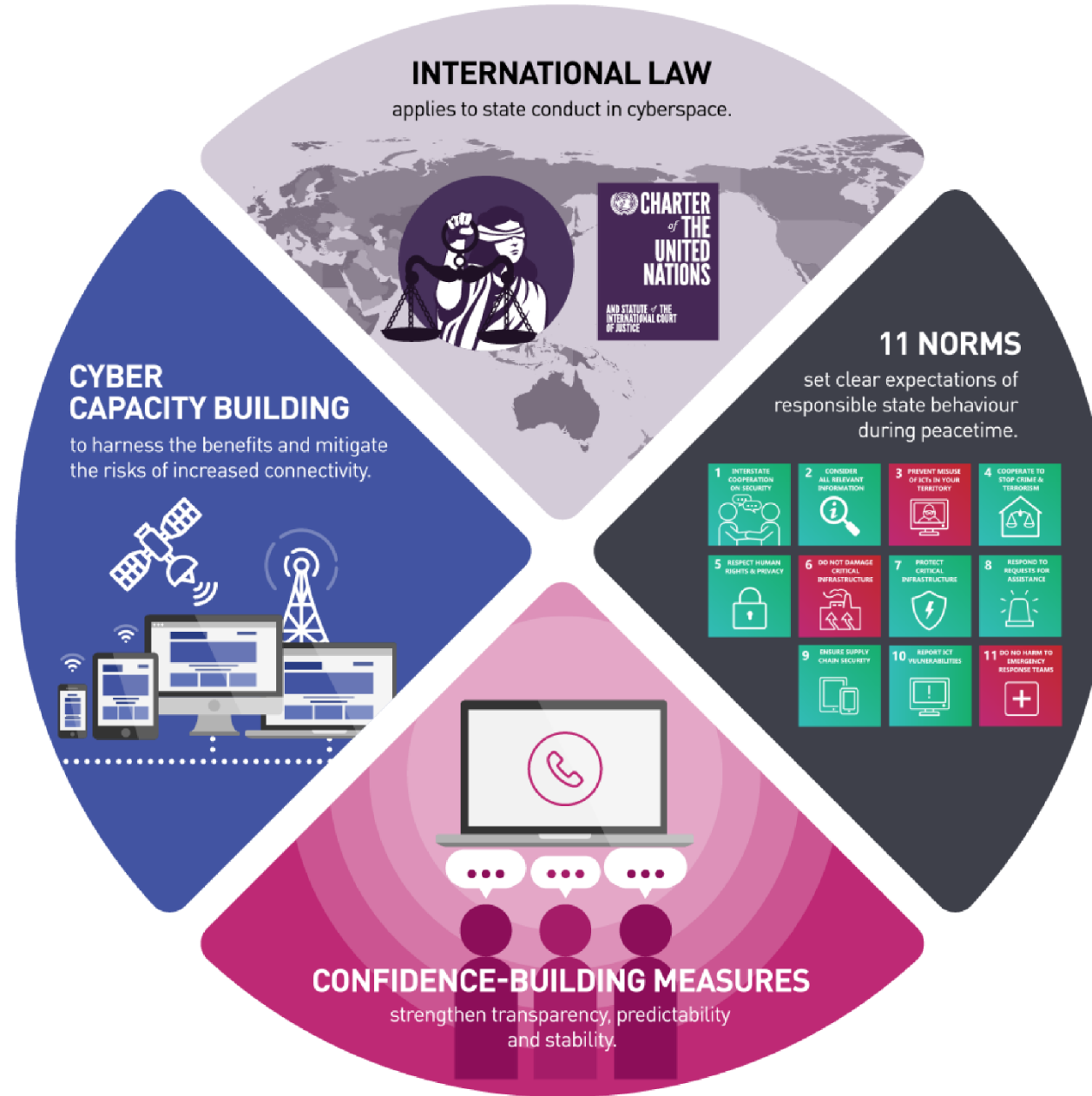


The Tech Accord welcomes the GCSC norms - special reference to **norms to avoid tampering, against commandeering of ICT devices into botnets, and for states to create a VEP**

**Find & download our report "Advancing Cyberstability"**

- [www.cyberstability.org/report](http://www.cyberstability.org/report)

**Read, Understand, Internalise, Practice, Champion and Own the Principles and Norms we have articulated – they are yours.**



**Tallinn Manual 2.0 is the updated and expanded second edition of Tallinn Manual on the International Law Applicable to Cyber Warfare.**

<https://ccdcoe.org/research/tallinn-manual/>



## **Inclusive Digital Economy & Society**

## **Human and Institutional Capacity**

## **Human Rights & Human Agency**

- **Capacity to act**, especially in a moral manner

## **Trust, Security & Stability**

- Development of a Global Commitment on **Digital Trust and Security** to shape a shared vision, identify attributes of digital stability, elucidate and strengthen the implementation of norms for responsible uses of technology, and propose priorities for action.

## **Global Digital Cooperation**

**The Age of Digital Interdependence: Report of the UN High-Level Panel on Digital Cooperation** <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf>

## Comparative Survey

of the two UN-based processes on responsible behaviour in cyberspace



### UN GGE Report 2010 (Res. A/65/201)

<https://dig.watch/instruments/un-gge-report-2010-res-a65201>

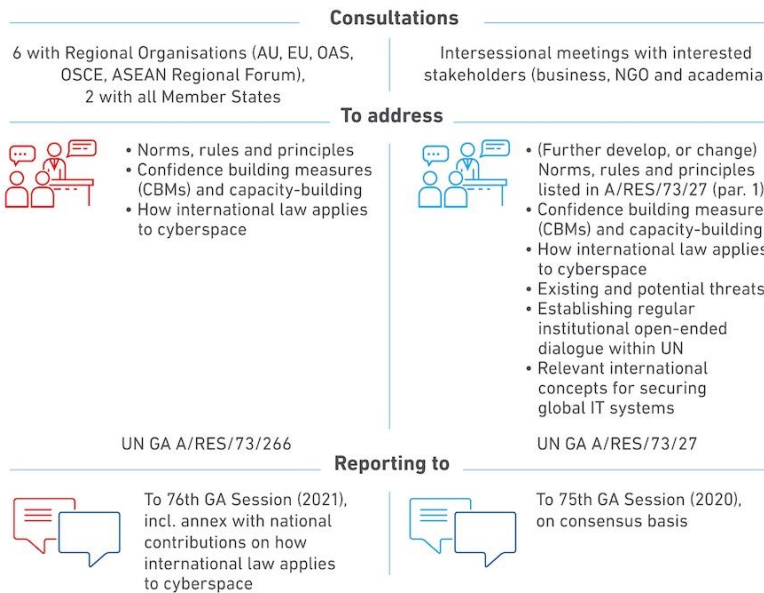
### UN GGE Report 2013 (A/68/98\*)

<https://dig.watch/un-gge-report-2013-a6898>

### UN GGE Report 2015 (A/70/174)

<https://dig.watch/un-gge-report-2015-a70174>

### UN GGE Report 2017 No Report

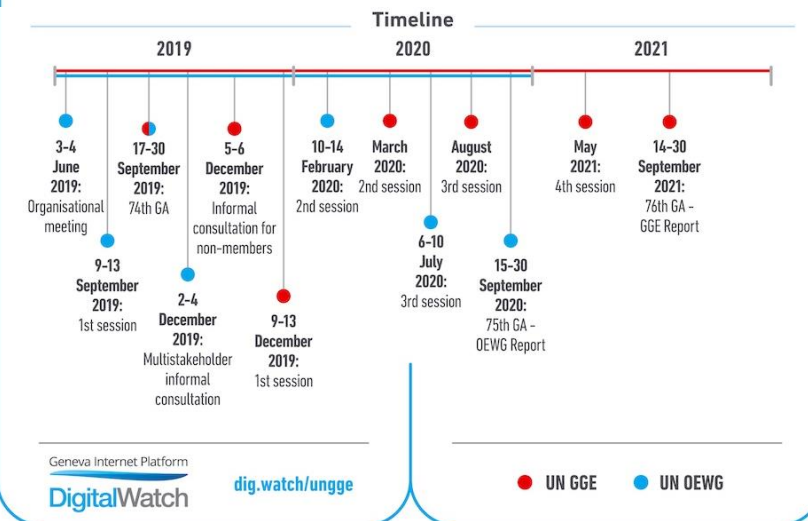


## UN GA Resolution on establishment of OEWG (A/RES/73/27)

<https://dig.watch/instruments/un-ga-resolution-establishment-oewg-ares7327>

## UN GA Resolution on establishment of GEE in 2019 (A/RES/73/266)

<https://dig.watch/instruments/resolution-ares73266-advancing-responsible-state-behaviour-cyberspace-context-international>





**Norms are “a collective expectation for the proper behaviour of actors with a given identity”**

Actions that the main stakeholders in cyberspace can take **during all stages of a (latent) conflict** with the aim of reducing and eliminating causes of **mistrust, fear, misunderstanding, and miscalculation** that may stem from the use of ICTs



States are encouraged to have in place **national legislation to facilitate on a voluntary basis bilateral co-operation and information exchange between**

- competent authorities,
- including law enforcement agencies,
- in order to counter terrorist or criminal use of ICTs;



States will nominate a **contact point**

- to facilitate pertinent communications and dialogue on the security of and in the use of ICTs,
- voluntarily provide contact data for existing official national structures that manage ICT-related incidents
- co-ordinate responses to enable a direct dialogue, and
- facilitate interaction among responsible national bodies and experts.



States will **voluntarily share information** on their:

- National organisation,
- Strategies,
- Policies and
- Programmes,
- including information about co-operation between the public and the private sector relevant to the security of and in the use of ICTs;



States will, in order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, as a first step, **voluntarily provide a list of national terminology related to the security of and in the use of ICTs**, accompanied by an explanation or definition of each term;




Intent was to conduct the **first information exchange** by **October 31, 2014**

CBMs are helpful in:  
**achieving predictability**  
 seeking clarification  
 gaining time  
**creating understanding**  
 enhancing maturity.





- **Voluntary and non-binding**
- **Contextualisation**
- **Operationalisation**
- **Harmonisation & Alignment**

In the context of ECOWAS and the AU	UN Norm 1: Interstate Cooperation on Security	
What are examples of implementation?	Examples of good global practice	What are Proper Questions for Benchmarking
<p style="text-align: center;"><b>Tactics</b> (What is my country/ region doing?)</p>	<ol style="list-style-type: none"> <li>1. Cooperation in regional arrangements (AU, ECOWAS &amp; other Regional Fora)</li> <li>2. Participation in UN GGE and OEWG</li> <li>3. Bilateral Dialogues</li> <li>4. Cyber points of Contact Directory</li> </ol>	<p style="color: red;"><b>Is my country represented in relevant multilateral and regional fora that deal with cybersecurity issues?</b></p>
<p style="text-align: center;"><b>Tools</b> (How my county is doing it?)</p>	<ol style="list-style-type: none"> <li>1. Cyber Affairs unit at the Ministry of Foreign Affairs</li> <li>2. International units at the National Cybersecurity Centre</li> <li>3. Develop international standards for emerging technologies</li> </ol>	<p style="color: red;"><b>Does my country have the means and capabilities for international engagement?</b></p>
<p style="text-align: center;"><b>Procedures</b> (Why my country is doing what it does)</p>	<ol style="list-style-type: none"> <li>1. International cyber diplomacy strategy</li> <li>2. <b>National cybersecurity strategy</b></li> <li>3. Speeches and statements from cabinet members</li> </ol>	<p style="color: red;"><b>Does my country have a strategy that guides our international cooperation in the form of articulated principles, vision and objectives?</b></p>



**African Union  
Cybersecurity Expert  
Group (AUCSEG)**



???



**Cybercrime Advisory  
Council?**

UNODA CYBERDIPLOMACY COURSE: FURTHERING  
THE PEACEFUL USE OF ICTS

[www.disarmamenteducation.org  
/index.php?go=education](http://www.disarmamenteducation.org/index.php?go=education)

- **Cost: Free.**
- **Anyone can enroll.**
- **Certificate:** The participant will pass by completing the online training course.
- **Upon completion the participant will be awarded a certificate of completion.**

### What is OIC-CERT

- [www.facebook.com/CS2Nigeria/videos/2500074973652382](https://www.facebook.com/CS2Nigeria/videos/2500074973652382)

Diplo  
online  
courses

- <https://www.diplomacy.edu/courses>

Diplo  
Course  
Titles

- **Artificial Intelligence**
- **Bilateral Diplomacy**
- **Diplomacy of Small States**
- **E-Diplomacy**
- **Internet Technology and Policy**
- **Multilateral Diplomacy**
- **21st Century Diplomacy**
- **Diplomatic Law: Privileges & Immunities**
- **Economic Diplomacy**
- **Language and Diplomacy**
- **Development Diplomacy**
- **Cybersecurity**



**Thank  
you, for  
your  
attention**

**Na gode,  
don  
kulawa**



**O ʒeun,  
fun  
akiyesi re**

**Na-ekele  
gi, n'ihhi na  
gi na anya**