International Norms in Cyberspace: Practice and Exploration Forum

Speech
WIC summit 2025 sub forum international norms
By
Nii Quaynor

WIC summit 9:00-11:00,
November 9, 2025
Yudu conference room

Your Excellencies, Ladies and Gentlemen, it is a pleasure for me to speak at the international norms forum to contribute to discussions on topic
“Cyberspace
Order and Security.”

I’ll introduce the community ecosystem in the region, make an effort to characterize cyberspace, point to current governance structures and conclude with cybersecurity matters.

The regional technical organizations in our ecosystem, af*, include resource management numbers registry (Afrinic), network operators capacity building (AfNOG), research and education networks(Afren), name registries (Aftld), Dotafrica registry, registrars(Afregistrar), and emergency response teams (Africacert) all of whom seek to deepen digital cooperation. These organizations share

common objective of connecting Africa and to connect to global. They coordinate their activities to build better Internet in the region and are core elements of governance in the region.

Let see what defines cyberspace, the challenges it poses, how things have been managed and how to evolve with focus on security.

We consider

“Cyberspace is a global and dynamic domain (subject to constant change) characterized by the combined use of electrons and the electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share, and extract, use, eliminate information and disrupt physical resources.”

Much like digital non tangible objects and resources came with new challenges, the Cyberspace

defies the established rules and principles of the existing (old) International relations with new attributes and requirements. It operates in the near-real time, goes beyond geography and physical locations, transcends jurisdictions and borders, enable activism and political expression, obscure identities of actors and links to action and does not follow existing structure of accountability.

Even though the cyberspace goes far beyond the Internet, the internet has shaped its existence for the last 5 decades. The global ubiquitous Network of Networks based on TCP/IP has changed the way the world exists, operate and is governed.

After the Cold War ended, businesses built an interdependent global economy on top of largely U.S.-centered infrastructure. The United States' technological platforms

—the Internet, e-commerce, and, later, social media—wove the world's communications systems together.

Originally funded by US government, the Internet was moved to the commercial world and became used globally. US government recently transfers the oversight over the IANA functions to the community through ICANN. Internet became fully governed by

bottom-up and multi-stakeholders' model.

Internet governance is organized through the Internet protocols, the number resources, and the naming and root servers' system.

The governance of the cyberspace has been subject for many conference, world summit on information society (WSIS), world conference on international

telecommunications (WCIT), world inter conference (WIC), internet governance forum (IGF), etc…

While in other realms, state actors play visible roles, they count as stakeholder under the MS model and are given specific role or mandate in some cases. ICANN's Governmental Advisory Committee (GAC) is an example. The Internet has consolidated around few big

techs company, some too big to be regulated by states. Majority of these are non-state actors.

Apps stores and closed devices, client capture, sticky services, etc. from one side, tight regulation, censorship and content control from other side.

The debate has been inflating about the roles and responsibilities of the state actors versus non-state actors.

Cybersecurity has been a hot topic. The ecosystem has reacted by adapting existing rules and designing solutions to the new threat inherit to the cyber domain. Multi-stakeholders' approach have been advocated with strong need for collaboration and cooperation. CERTs, CSIRTs, national cybersecurity are established. International treaties and conventions are adopted to frame the responses to cyber threats and fight cyber

criminals. The Budapest convention on cybercrime of the council of Europe is the well-known one. In 2014, African union adopted the African Union convention on Cyber security and personal data protection (Malabo convention) which is still ongoing with member states implementation.

Cybersecurity ecosystem evolved rapidly with various uncoordinated actors (state and non-state) with conflicting

agenda and methods, rendering the actions and solutions less efficient and a poorer cybersecurity as result.

Cyberspace is shifting the conflict and control panel to digital espionage, cyber threats, cyber wars, etc. calling for cyber defence and new alliances.

Despite the efforts, according to the ITU Global Cybersecurity Index, many countries still have

a significant cyber-security gap. This gap is more important in the developing and low-income world.

The emerging technologies come with opportunities and threats. It is likely these technologies will exacerbate the cyber risks.

Current response and approaches showed their limits. The world has not succeeded in matching the traditional

approaches to theory and research, practice, and policy as derived from experiences in the 19th and 20th centuries, to the cyberspace.

Internet was designed based on trust but adapted and adjusted as it evolved and faced by a hostile ecosystem. Its global and distributed nature, coupled with the backward compatible and incremental requirements challenges the needs for a

strong secure and safe cyberspace.

The security in the cyberspace requires technological and scientific solutions but also socio-economic, political and regulatory solutions which involve different actors.

The emerging technologies bring new actors, new uncertainties to which the cyberspace is not well prepared for.

New methods and solutions are required to deal with real-time, boundaryless and permeation, fluidity, attribution and accountability challenges in the cyberspace.

The opposition between generative and reductive models, between heavy regulation and light regulation must be given due consideration in the global context when

discussing cyberspace order and security.
The race for new technologies will not ease things.

Africa where I come from and the global south in general should have voices not as users or observers, but also as active actors and partners. The seats will have to be earned and not granted.

I thank you for your attention