WIC summit 2025 main forum speech
By
Nii Quaynor

WIC summit 14:30-17:00, November 7, 2025

Your Excellencies, Ladies and Gentlemen, it is a pleasure for me to say a few words to the distinguished audience at the Summit to contribute to discussions on topic “Forging an Open, Cooperative, Secure and Inclusive Digital Future - Building a Community with a Shared Future in Cyberspace."

We are creating an Inclusive and secure Cyberspace Beneficial to All

I come with warm regards from the engineering and academic communities in Africa and thank you for opportunity to share these views today.

The African Internet technical community held its 2025, African Internet Summit from 30 September- 3 October 2025 “themed : A resilience Internet Ecosystem for an innovative digital Africa”, and are most grateful that the Secretary General of WIC, H.E. Ren Xianlian, was able to participate and address the opening ceremony. His statement encouraging Africa to do more on its own and to work in local languages, was a powerful message that resonated with the community. We appreciate Secretary General’s thoughtful message and thank WIC for engaging with Africa’s technical community which had gathered to celebrate 30 years of Internet, reflect on the journey, the challenges and opportunities for a better digital Africa.

I am also glad to have had a opportunity to speak at WIC Open Forum at UN IGF held in June in Norway, on theme of

“Bridging the Digital Divide – Focus on the Global South”, where I shared views and perspectives on how Africa can be supported in order to embrace the new and emerging technologies. This shows the close collaboration of WIC with the African technical community and we look forward to welcoming WIC at next WIC Africa meeting.

I’ll introduce the community ecosystem in the region, comment on development efforts in the region on internet infrastructure and conclude with governance around services from infrastructure.

The regional organizations of 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.

We are developing the cyber space from name and number identifiers, voluntarily adopted by users and providers creating a Domain Name System. These identifiers belong to community and are used to serve a large continental area. These resources are not assets and do not belong to providers nor to registries.

Emerging Internet communities like Africa appear fortunate with open practices that give us a chance to be involved globally. The open standards, open documentation and open participation have been helpful in building capacity. This ease of development may have become our new problem with Internet consolidation on few USA based providers

We inherit two types of security governance: the security arrangements around infrastructure and governance of behavior of users of services.

The security of infrastructure best managed by standards, best practices, regulation of operators and technical capacity. The approaches here are multi stakeholder and more bottom up community discussions. The MS and bottom-up approach have been abused in the ongoing challenges with the number registry…

Like the Internet, the registry core functions have shown resilience and there are lessons learnt to improve the governance and best practices.

The governance of behavior of users is subject to laws and global norms. Coordination at UN, national and local levels are the result

We encounter sufficient cybersecurity challenges among users of domain names. We are reminded to pay attention to cryptography and appreciate, multi factor authentication and zero trust as best practices for a safer internet. Africa is expected to be implementing these recommended practices and need to invest in cryptography development as part of infrastructure. With number resources meant for a region’s development, prevalent out of region use of IPs would be a security governance concern.

There are three potential AI divides we should pay attention to. Firstly, technical capacities and educational preparedness for adoption needs to improve to avoid divide. Secondly, the costs of equipment and infrastructure for training AI imposes an economic divide on participation on supply side of AI. Lastly, the electrical power to run these machines limits ability to participate beyond user level.

We are encouraged by technical cooperation opportunities on global security governance through WIC and looking for technology transfer to our region.

We continue to deepen our foundation to cope with the emerging technologies and how to manage with our limited resources yet able to be on the supplier chain… to be part, contribute and be heard. Together, we build a community with a Shared Future in Cyberspace and gain mutual benefits in development.

Thank you for your attention