

Questions – Answered- U.M. Mbanaso PhD

1 How does good cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Safe and secure Cyberspace will no doubt bolster Sustainable Development Goals (SDGs). Cybersecurity will provide the enabling trust and confidence for netizens to use the Internet technologies for emancipation and prosperity. Providing Cybersecurity requires three tightly coupled layers:

- i. The individual fully aware and responsible for the protection of that part of Internet Technologies he/she is in charge of;*
- ii. The Corporate entity full aware of its role and responsibility for the protection of the Internet Technologies that it either provides and/or uses;*
- iii. The Country fully aware of governance issues and roles in both technical, legal and institutional responsibilities.*

2 How does poor cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?

Poor cybersecurity will undermine the growth and trust of Internet Technologies as it will unwittingly discourage netizens from the use of Internet space.

3 Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges?

Policy and strategy are a vital components of effective cybersecurity. It foundationally set the parameters for effective Internet governance. A well-crafted policy set sets the direction for regulation, compliance and conformance.

4 Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services

5 Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfil critical goals such as payments.

Mobile devices are fast revolutionising the landscape of Internet space and as a disruptive system having almost all characteristics of computing device, must be highly secure.

6 Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended.

Authorities of state should support and promote Open Internet, safe and secure cyber environment, consider strong regulation as opposed to censorship.

7 Confidentiality and availability of sensitive information, in particular in medical and health services

Software applications that process sensitive information must have security baseline that take into cognizance the various layers and applicable security controls. Such applications must repeatedly be certified by relevant certification agencies to confirm that baseline security is being applied.

U.M. Mbanaso PhD

I am currently, the Executive Director, Centre for Cyberspace Studies, a visiting academic at the LINK Centre, Wits University, South Africa. I was vigorously involved in the drafting of Nigeria Cybercrimes Act 2015, National Cybersecurity Strategy and Policy 2015, and many other Cybersecurity framework development in Nigeria. Prior to joining Nasarawa State University, I worked with the public sector for twenty five years during which I actively functioned in providing cutting edge ICT solutions. I earned undergraduate qualification in Electronic and Communications Engineering from Nigeria, MSc in Information Technology from the UK, and PhD Information and Communications Security from the UK. I have delivered outstanding Cyber – related and operational intelligence papers to conferences, workshops, seminars, etc. as well as significant number of publications to his credit. I am a member of ISACA (USA), IEEE (USA), The Institution of Engineering and Technology (IET), UK, Nigeria Computer Society (NCS), Computer Professionals Registration Council of Nigeria (CPN) and EC-Council member.

The Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria is the first multi-disciplinary centre in Nigeria, established to carry out R&D, develop and build vital e-skills for the rapidly changing cyberspace. The Centre has continued to develop relationships and collaborate with various cyber-focused research, education, and training communities within the African continent and other relevant research groups across the globe. The Centre's activity focuses on the general area of Cyber development and governance that span cybersecurity, cybercrime, regulation and compliance, social media networking as well as emerging disruptive technologies.

My research interest span the spectrum of Cyberspace, focusing on cyber security, governance, innovations, intelligence and technical.