An intelligent approach to building sustainable cyber resilience for states in Africa against cyber-terrorism.

The growth of the cyber space in recent time has outperformed any other commodity of development. It is a major part of the growth of any country as over three billion people in the world today are connected to the internet through cyberspace. However, It's potential growth is estimated to hit five billion people with over fifty billion devices connected by 2020. According to a report by ITU in 2014, the fastest growth is experienced in developing countries majorly in Asia and Africa. With rapid growth is accompanied by new vulnerabilities, risk and challenges. One of these challenge is Cyber terrorism. Wikipedia defines cyber terrorism as "deployment by known terrorist organization of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption". This attacks range from cybercrime, malware on infrastructures owned by states, organizations and individuals. The recent 2016 presidential elections in the US buttresses this phenomenon as many observers argue that the outcome of the elections were interfered by Russians. Also in 2017, over 145 million customer's loss their data on Equifax, one of US largest credit bureaus.

Statistics has shown that cybercriminals consider Africa as potential space for their act largely because of its overall economic growth performance with massive internet inclusion and for its porosity to cyber-related threats. Africa development Bank (AfDB) claims that Africa economies are rated among the world's fastest growing economies as seen in the continent's increasing middle class and acceptance of mobile technology. Norton Cyber-Crime reports that South Africa ranks third highest with 80% of cybercrime victims in the world after Russia and China with 92% and 84% respectively. Also, the Symantec report deepens this assertions revealing that the number of sponsored cyberattacks in Africa grew by 42% in 2012, highlighting that 31% out of the 42% were categorized as cyber espionage. We have also seen reports from the investigations on the attack of the Westgate Mall in Kenya, the ruthless acts from Boko Haram in Nigeria and AQIM (Al-Qaida in Islamic Maghreb) in Northern Africa; that these groups leverage on cyber infrastructure to recruit, plan, coordinate and implement their attacks. A recent report from the Nigerian defense headquarters stated that Boko Haram used social media for recruitment and was responsible for the defacing of their website and the website of the National Electoral Commission (INEC) during the 2015 presidential election. Many cases are not even reported, it is well accepted in the intelligence community that terrorist groups around the world now use the internet with encrypted data to communicate, making it difficult for law enforcement in developing countries to intercept their messages. The Economic Commission for Africa (ECA) recently reported that a survey on 21 countries revealed that while many countries in Africa had proposed legislations, the level of implementing and deploying security systems to combat cybercrime in the public and private sector was low.

It is therefore, expedient to step up actions to build intelligent cyber-capabilities with the aim to monitor, defend and protect the cyberspace and its infrastructure through distributed denial of service attacks (DDoS) on criminals and terrorist groups in Africa.

Cybersecurity is at the core of the development of the economic, social, political and individual safety of all nations in Africa and should be prioritized in its developmental agenda. Establishing cyber resilience exceeds creating barriers from attackers, it also requires setting up dedicated intelligent processes necessary for the management of cyber crises in the states of Africa.

Recently, I was privileged to support a cyber-security contractor to build a cyber-mechanism using big data and artificial intelligence technologies for a top intelligence agency in Nigeria to track and intercept the cyber activities of Boko Haram operatives. This was a huge success as it intercepted over 223 plots between 2017 and 2018. Saving hundreds of lives and several millions of dollars. As stakeholders we came to realize that this investment in securing cyberspace also affects the success rate of other policy initiative as well. African states can build cyber resilience by integrating cyber risk protection and crisis management in their decision- making process by preparing for cyberattacks with mitigation plans. Cases of spreading fake news on social media can be tracked from the root distributor and diffused quickly using intelligent cyber-mechanics before its negative impact affect millions of vulnerable lives.

States in Africa can build their cyber resilience strategies by

1. Establishing a dedicated Cyber Counter-terrorism centers using cutting edge technologies such as big data and artificial intelligence required for effective surveillance, proactive detection and rapid response as seen in the recent establishment of the Nigerian
2. Improve on their national cyber strategies and policies including adapting with recent technological trends.
3. Accelerate the knowledge of cyber-skills in the public and private sector through public private partnerships and cyber-cohort programs.
4. Promote responsible cyber culture and education in every sphere of the society.
5. create or improve responsive legal and regulatory frameworks that do not prevent innovation
6. Set new standards such as privacy protection for citizens for all cyber services and mobile products within their jurisdiction.

These are essential in achieving a nation's security developmental goals, as it greatly eradicates the digital security risk resulting from access to and use of the cyberspace. More than ever before, nations of Africa will need to align their cybersecurity objectives with their strategic national ambitions with the aim to unlock the prosperity inherent in the space while protecting the sovereignty and integrity of their critical infrastructure as they build resilience against cyber terrorism.

It is time to act. And the time is now!

Prince Ogbonna.