02nd July 2021

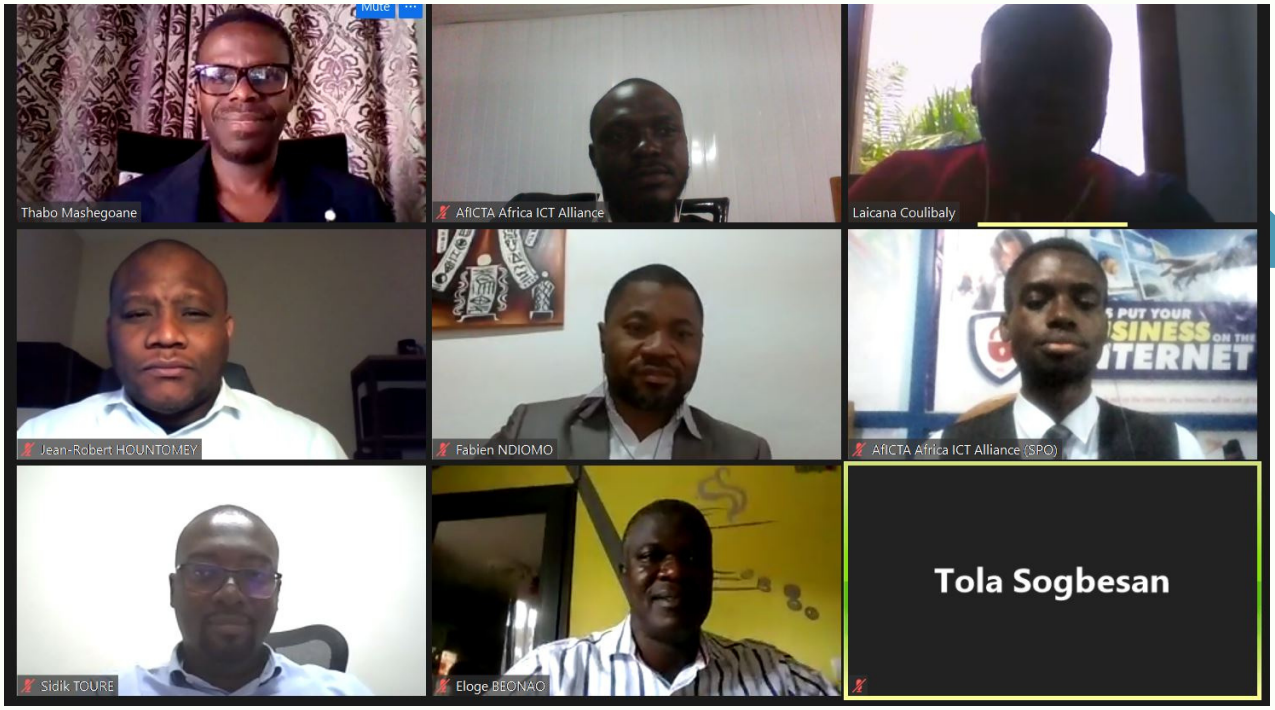
AfICTA Quarterly Webinar Report

29th June 2021

"Cybersecurity Innovation: How Africa Can Contribute"

On 29 June 2021, AfICTA in collaboration with Diamond Security Consulting organized the 2nd edition of its Quarterly series on "Cybersecurity Innovation: How Africa Can Contribute?"
It provided a platform for professionals from across Africa to share knowledge on the necessary proactive solution that can be deployed to increase Africa's contribution on the Cybersecurity & Innovation front. and more spec ways to protect and secure our digital identity.

The webinar was a very successful one with panelists and participants from all over Africa online who enriched the collective discourse. Among the highly esteemed panelists are: **Cheick Omar OUEDRAOGO**, Deputy General Manager of Talentys Burkina Faso; **Sidik TOURE**, Program Director, Banking and Critical Services Security, Orange Middle East and Africa; **Eloge BEONAO**, CIO, MTN Côte d'Ivoire; **Jean-Robert HOUNTOMEY**, Director, AfricaCERT; **Fabien NDIOMO**, Regional Information Security Head WECA of MTN Group



Opening Remarks

Mr. Laicana Coulibaly, CEO of Diamond Security Consulting and board members at AfICTA was the lead facilitator of the webinar. He welcomed all participants to the session and thanked everyone for taking the time to partake in the webinar. He also announced all the speakers on the call before introducing the Vice-Chairman East Africa Region, AfICTA, and host of the webinar to give an opening welcome speech and introduced the Chairman for the brief opening remarks for AfICTA.

Mr. Thabo Mashegoane, opened by thanking the panelists for their time and expertise, welcomed the participants, and proceeded to buttress the importance of the theme of the webinar which is very imperative in the post COVID world which saw exponential growth in the Cyber threats due to the rapid Digital adoption in the new age. The spike in cyber threats not only creates a demand for cyberthreats solutions but also creates a market for cyber innovators and the theme of the webinar would focus on the Afrocentric approach to meeting the demands pertaining to the specific context of the African Cyber Ecosystem. He then introduced the moderator for the panel session, Mr. Laicana Coulibaly.

Africa's contribution currently to the global cyberspace ecosystem

Mr Laicana posed the first question on Africa's contribution currently to the global cyberspace ecosystem and Mr. Cheick Omar shared his opinions from the microscopic analysis of the francophone countries in Africa. Although the recent pandemic times have resulted in an increase in general digital adoption there isn't any significant interest nor contributions in the cybersecurity innovation because stakeholders still inherently hold user-centric views on the benefits of adoption. The best way to address this is through constant and sustained awareness at all levels to ensure there is increased interest in the field. Cyberthreat agencies across the continent are either non-existent or dysfunctional and this needs to be addressed quickly albeit there is a lack of resources for this sector but the market created by the sector is very massive and could also be an avenue for job creation across the continent.

Jena -Robert from AfricaCERT held a more optimistic view that although more works need to be done on the continent in terms of developing solutions and strategies that aid mitigation of cyber threats they also need to be commended so far on the continent as more countries are now creating cybersecurity policy frameworks and in some cases capacity development schemes in the sector. According to the research from AfricaCERT working rigorously to stimulate development through close efforts with the African Union and other National Agencies, ECOWAS now has developed a global Cybersecurity for all countries in the region of the West African states. As of last year, 21 Incident Response teams were set up in the continent and now there are about 27 which indicates the growing efforts in the area albeit there is still a need for more resources and capacity building within these agencies and organizations.

African Nations are participating in the UNDG & UN Open-Ended Working Group discussion on Cybersecurity which means there is a growing appetite for application security, product security, and issues related to investigation availability and disclosure. The naming Industry has also made very significant strides through vertical collaboration across African Countries such as the Cyber drill exercises organized between CIR organizations and National partners

Responsibilities of Private Public Sector in Cybersecurity Innovation

There is a need for the public sector to create the guidelines and platforms that engender Cybersecurity innovation and solutions by ensuring all stakeholders in the digital economy ecosystem are held to specific security standards that are not to be bridged. In North Africa, policies that require regular assessment tests, notification, and reporting of incidences are established and implemented which shows that there is also a need for more vertical collaboration and sharing of best practices such as the aforementioned to engender cybersecurity awareness and growth in other parts of the continent. The major reason for the lack of implementation of these cybersecurity standards and policies is due to the lack of investment and resources provided in terms of expertise and capacity and investigative technologies. The private sector needs to priorities cybersecurity by providing norms through knowledge sharing on best practices.

Currently, it's no myth that there is little to no investment from the different stakeholder groups on the development of Cybersecurity solutions based on our realities.

Only a few fortune 500 companies take the mantle and try to meet world standards by investing in solutions in Africa. In other, for this to change, then there needs to be more public-private partnership that aims at investing in infrastructure, capacity, and market research.

Cyber standards based on our Realities?

Although there is a need for adaptation of global standards based on the socio-economic realities in Africa, global standards are available for certain reasons, primarily for more synergy. Notwithstanding, there is a need for cybersecurity frameworks based on the African context, but we must ensure that we don't deviate from the "global truth". We may create policies and standards that prioritize the African socio-economic realities, the collaboration between all stakeholder groups has to be implemented to ensure that these standards are understood by everyone involved. It may be more beneficial for African teams to join global standard-making bodies to ensure we contribute and table our needs at standard and policy discussions rather than desolidarizing by creating ours

Cybersecurity and Digital Sovereignty

Does the road to Digital Sovereignty pass through Innovation in Cybersecurity?

A major discussion at the European Union is the matter of digital sovereignty, the growing penetration of technology also indicates the need for digital sovereignty in Africa. it is clear that technology really reforms how people interact and this is exemplified with the boost in digital users in Africa. For us to begin to have control over the way our data is utilized, then we need to begin to think of how we can become creators and not just consumers of cyber technologies because so long as someone else creates for you then it is impossible to control or manage how your data is utilized. In other to migrate to being creators of cyber technology as opposed to just consumers, a mental shift from all stakeholder groups is imminent so matters of cybersecurity are prioritized as a matter of Security not just for cyberspace and the major step in this direction would entail creating budgetary allocation at all levels for Cyber solutions and technologies.

How can Africa create Cyber solution on the Gartner Magic Quadrant?

It isn't totally out of the realm of possibility for Africa to create solutions on the Gartner magic quadrant. We know that we are blessed with a plethora of talent on the continent and even with the limited resources on the continent, we find that some organizations are still competing at the international level, but all barriers that hinder growth has to be dismantled and then an enabling environment that spurs innovation has to be created and this is only achievable through collaboration between the public and private sector. The African diaspora also has a role to play if we intend to grow. Collaboration between Africans on the continent and in the diaspora is very imperative and this should encourage the diaspora to bring the solutions home as well. The tradition of open-source solutions needs to be cultivated strongly as this could Fastrack our contribution to the cyber innovative landscape.

Q & A Session

How do we encourage our Public Leaders to take leadership in Cybersecurity seriously viz-a-viz putting regulations and laws in place considering that only 8 of 55 countries have Cybersecurity Strategies?

Cyber capacity building as defined by the global forum for Global Forum on Cyber Expertise (GFCE) has 4 pillars:

1. Policy and Strategy: interested in National Strategy Assessment, Confidence building measure norm & Cyber diplomacy & international law in cyberspace.
2. Incident Management & Critical Infrastructure Protection: interested with National Computer emergence & Security Incidence Response teams, Cybersecurity exercise and Critical Information Protection.
3. Culture & Skills: interested in Cybersecurity assessment, Education, and Training, and Workforce Development.
4. Standard: interested in the promotion of internet-related standards. The GCFE works on having constant constructive dialogue among multi-stakeholder groups to set the agenda to drive Cybersecurity development. The public sector needs to be held accountable o implementing all the schemes and programs put forwards a dialogue such as the current webinar. We need to build on existing frameworks for Cybersecurity development and ensure that the public is invited to constructive dialogue both at the national and global level to ensure accountability at all levels.

Are private sector associations or groups relevant in enhancing Africa's positive contributions to the African / global Cybersecurity ecosystem?

Although there are groups that are intended the do this, most of these companies are rather interested in how Cybersecurity policies and contributions can enhance their business rather than on how they can contribute to the global ecosystem. Another issue is that although buttresses the need for priorities of Cybersecurity there are still very minimal organizations that are specifically established to address issues and matters of cybersecurity, hence the reason for more awareness of the market and benefits for entities from the private sector to invest/. Lastly, the contributions of the private sector are closely tagged with the policies of the public sector and so in other for one to grow then policymaker must play their parts as well taking the initiative to create policies that necessitate the need for public counterparts to adhere to and be more involved to in turn such contributions in the cybersecurity ecosystem.

You can view recording here: https://youtu.be/VoL2CekXI6wA