AfICTA 11TH QUARTERLY WEBINAR

26TH APRIL 2023

Prepared by AfICTA Secretariat

“Cybersecurity in West Africa: Exploring the UNECA Insight”

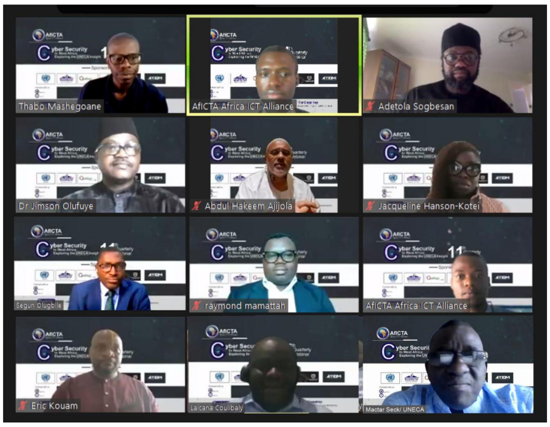
On 26th April 2023, AfICTA organized 11th edition of its Quarterly webinar themed "Cybersecurity in West Africa: Exploring the UNECA Insight”

The platform availed professionals across West Africa region to share knowledge and best practices on cybersecurity and its challenges in West Africa.

The discussions were geared towards the importance of awareness creation, how to invest heavily in Cybersecurity architecture, encourage cybersecurity career uptake, promote cybersecurity best practices, conduct regular cybersecurity training and manage/report breaches when they happen.

The webinar was a very successful one with panelists and participants from West Africa region and beyond who enriched the collective discourse. Among the highly esteemed panelists were Dr. Mactar Seck, the webinar Chair and Economic Affairs Officer at UNECA; Dr Jimson Olufuye, the lead researcher for CD4IR and Principal Consultant for Kontemporay Konsulting Ltd; Ms. Jacqueline Hans Montei, MTN Ghana’s Security Head and the Senior Manager for Enterprise Information Security & Governance; Mr.Eric Kouam, Consulting Director and Founders of QUALISYS Consulting; Mr. Laïcana Coulibaly, CEO & Founder of Diamond Security Consulting; Mr. Raymond Selorm Mamattah, Founder and President of the E-Governance and Internet Governance Foundation for Africa (EGIGFA); Abdul-Hakeem Ajijola (AhA), Chair, Nigerian National Cybersecurity Policy and Strategy review committee & Chair, Nigeria Computer Society, Cybersecurity Advisory Group; and Amb. Segun Olugbile, CEO, Araba Technologies.

Mr. Adetola Sogbesan, AfICTA , Vice-Chairman, West Africa, was the lead facilitator of the webinar. He welcomed all participants to the session and thanked everyone for taking the time to participate in the webinar. He highlighted that the purpose of the webinar is for knowledge sharing on mechanism for ensuring online safety from the perspectives of different regions in the continent. He then welcomed Mr. Thabo Mashegoane, Chairman, AfICTA for his opening remarks.



Chair opening remarks

Mr. Thabo Mashegoane, opened by thanking the panelists for their time and expertise, He also welcomed the participants and proceeded to buttress the importance of the theme of the webinar which is very imperative as the core of digitalization is rapidly transcending. He noted that the webinar topic lies in the core of a lot of challenges with regards to the change we are on, and also the bridging that AfICTA got for making a digital promise to be delivered for everyone in Africa. He stressed that it is within that context that digital transformation as it were has been up-taken by a lot of people since the pandemic. And the focus and vision is for the numbers to grow and while the numbers are growing, we have to take cognizance that the mass adoption would also bring about increase in cases of attacks from nation-to-nation if no right measures are put in place.

From the research outcome, he made mention of a lot of correlation when it comes to cybersecurity and GDP of countries, the same correlation will also be seen when it comes to crimes vs GDP. He further highlighted that AfICTA as an advocacy group would continue to engage multi-stakeholderism approach in all its engagement within ICT ecosystem in the continent in combating cyberthreat He also indulge participant to engage and share perspective and finally extended his gratitude to all in attendance on behalf AfICTA.

After introductions of the panelists by Mr. Adetola Sogbesan, he yielded the floor to the webinar Chair, Dr Moctar Seck, Economic Affairs Officer at UNECA for his remarks.

The Chair of the webinar, Dr. Moctar Seck referenced the Webinar as one of the context of Africa digital agenda. He noted that the United nations has continued to take cybersecurity seriously through various initiative; the United Nations secretariat roadmap for digital cooperation has also stressed the importance of cybersecurity in the world. He noted that when it comes to Africa, there is a digital strategy put in place since 2020 as a projection toward 2030. He stressed that as African Countries, we need to ensure safe, and equal digital transformation especially with the AfCFTA - Africa Continent Free Trade Area initiative which serves as a digital tool and market to scale Africa's GDP as well as inter policy, intra regional trade initiative towards the digital Africa.

After UNECA representative's opening remarks, Mr. Adetola Sogbesan yielded the floor to the lead researcher for his presentation.

"Cybersecurity in the 4th Industrial Revolution"

Dr. Jimson Olufuye delivered a presentation on "Cybersecurity for Development in the 4th Industrial Revolution'. He highlighted that the research was conducted in 40 African nations (including 11 from West Africa Region) which showed that an increase of Cybersecurity maturity by 10% yields between 0.66% and 5.4% increase in per capita GDP in Africa. It was noted that the higher a nation's cybersecurity maturity, the lower the cyber financial loss per capita. Data from a sample size of the 40 nations under review also showed that a

10% rise in Internet Penetration enables between 1% and 8.2% increase in GDP per capita in Africa. The report also indicated that Africa's cybersecurity maturity is 29.1% compared to that of Latin America and Asia/Middle-East at 35.6% and 61% respectively.The outcome of the research recommends as follows; 1. Cyber security awareness and education effort at all enterprise/organisational levels should be enhanced. 2. There is a need for cybersecurity policy consistency and dedicated implementation of same in our countries. 3. West African countries at the ECOWAS level should evolve cooperation framework to mitigate cyber-risks in the sub-region. 4. They should also ascend to the Malabo Convention. 5. Efforts should be made to fast-tract the benefit realization of the African Centre for the Coordination and Research in Cybersecurity located in Lome, the Republic of Togo. 6. Periodic and consistent Information System Audit should be conducted on enterprise ICT systems. This is critical especially that government processes are being digitalized. Read more

Panel Session

After an impressive presentation by Dr. Jimson Olufuye, the facilitator then yielded the floor to the panelist. The adumbrated questions for justification was addressed to Ambassador. Segun Olugbile

- What are the factors responsible for Africa's lowest lost of revenue to cyber criminals? Does it mean we are doing something right? How?
  According to the research, Africa lost $19billion within the years reviewed, 75% of the lost is believed to have started with an email. What safety precaution should have been taken to avoid the loss?

Amb. Segun Olugbile responded that in recent data, Nigeria is presumed to be the biggest economies in Africa and ICT has contributed 60% of its GDP according to statistics from African Union, AU. He says there are vibrant financial institutions (FITC) in Nigeria which has helped in areas of cybersecurity programmes. The financial institutions has been vibrant in terms of investment and the rate by which the FINTECH are gearing on capacity building in the context of skill set and infrastructure has contributed substantially in curtailing cyber-criminality. He also noted that awareness creation on cybersecurity is on a high side which has helped in reducing such figures.

Panel Session

- In line with the UNECA research outcome which indicates that Africa's prosperity comes with it's own cyber challenges, how best can West African nations prepare to forestall these challenges?
- What approach is been adopted by MTN in Ghana in a joint force with government in reducing cyber attacks?

Ms. Jacqueline responded to the question aforementioned by highlighting key actions to be implemented on how West African Nations can forestall its own cyber challenges.

1. Fostering collaboration and information sharing, I.e collaboration between government and agencies, private sectors and other stakeholders like advocacy groups can help to identify and address measures in cybersecurity threat.
2. Government across West Africa nations should effectively put in place information security platforms and partnership to facilitate the

sharing of threat intelligence as well as best practices.

3. West Africa nations should develop a national cybersecurity strategy center which will serve as a focal point in coordinating cybersecurity efforts across various government agencies and private sector. This will also serve for monitoring and responding to cyber threat.
4. Government should pass cybersecurity laws and regulations to protect key critical infrastructure and sensitive data from cyberthreats. She emphasized that the laws will set standard for data protection by establishing penalty for cybercrimes, it will also provide guidance for incidence response and reporting.
5. Government and private sectors should encourage the promotion of platform for cybersecurity which will bring greater emphasis and enhancement.
6. Investing in cybersecurity infrastructure and technology. Government should come together with private sector to invest in infrastructure and technology to improve the ability to response to cyberthreat.

As a telecommunication company within the region, Ms. Jacqueline responded that MTN Ghana has partnered closely with the cybersecurity authority of Ghana as a joint force response against cyberthreat through, 1. Participation in workshop training on how to protect critical infrastructures, 2. Engaging Child online protection forum with civil societies organizations to discuss their role and the role of cybersecurity authority of Ghana, 3. Engagement with Internet World Foundation, META -Facebook which launched help the children campaign and safety online as Africa quota to step up the fight against distribution of child online, sexual abuse on the continent.

Ms. Jacqueline also noted that Child online protection discussion forum Organised by UNICEF is also part of the initiative. Knowledge sharing on cyberawareness which creates awareness among students in secondary schools on how to keep themselves safe and how to start a career in cybersecurity. Also media engagement was a key factor MTN uses in a joint force with government in reducing cyberattacks.

Panel Session

❖ 43 percent of cyber attacks target small businesses,

i. What safety precautions should such category of business and others do to ensure online safety?

ii. Considering that human error accounts for up to 87% of data breaches even in the region, what are the best approach to reducing the menace?

Mr. Eric Kouam highlighted some key loopholes that surrounds online safety across West African countries and one of the reasons are;

- Legal framework issue
- Policy framework issue
- Institutional mechanism issue

He noted that most countries despite having a national strategy for cybersecurity, those strategies were compiled by ministries incharge with little or no consultation of the stakeholders involved. Also noted that there is lack of coordination in the way of mobilizing different sector at the level of institutions.

He recommended that government at national level, financial institution and tech company should work together in having a national strategy. A strategy to bring together all stakeholders to be involved which will consolidate or enhance the expertise of others.

Panel Session

- In fast-tracking the prosperity of West African countries, strategies must be designed to connect the unconnected population. Do you think trust and safety are part of the issues delaying mass adoption of technology?

Dr. Jimson Olufuye responded to the aforementioned question that the issue around the delay of mass adoption of technology and connecting the unconnected is as a result of policy issue. That is, policy to use the universal service provisions funds effectively, and then ensuring that cost of deployment is reduced. He noted that Nigeria government is doing a lot, by ministries engaging the state so that the cost of right of way of deploying cyberlink, infrastructure is significantly reduced. He recommended that this should be scale through across all region which will enhance connectivity. On trust, Dr. Jimson Olufuye emphasized that the people trust the government to an extent because whenever government brings in a new service their is acceptance among the citizens. He also stressed that penetration data is really galloping up which means there is cybersecurity maturity embedded in a way in Internet penetration. Hence, recommended government needed to use those funding to provide the service.

Panel Session

- What are the cybersecurity "skills of tomorrow" that respond to the current challenges existing in the cybersecurity sector within the region and what are the incentives to ensure youths with the passion find them lucrative.

With regards to cybersecurity skills of tomorrow **Mr. Raymond M.** responded that the most important skill of tomorrow is social engineering skills. He emphasized that without social engineering skills, no matter the social mitigating strategies put in place, falling prey into social engineering tricks all the strategies put in place will be effort in futility. Hence, recommended the most important skills for both professionals and individuals is to have enough knowledge and skills on how to identify a social engineering tricks that is been deployed on a person and how to outweigh bad actors.

In response to making Cybersecurity profession more lucrative to youths , Mr. Raymond responded that African Countries belongs to the low income bracket due to its economic stance, hence, emphasized the necessity to make cybersecurity training and certification affordable. He recalled that most of the engagement with youth shows they are passionate to get more knowledge on cybersecurity and how to plugin to the profession but the cost serve as a constraint. He provided an entity in Africa that provides free certification and training in cybersecurity which is ***ICS2, adding that*** they are on a mission to get one million certified in cybersecurity across Africa.

Panel Session

- In the light of the outcome of the UNECA research on cyber security for development in the 4th Industrial Revolution which reported an increased in cyber attacks. How best can West African countries improve their cybersecurity architecture?

Mr. Laicana responded that cybersecurity in West Africa requires a collaborative approach, hence provided the underlisted recommendation on how west African Countries can improve its Cybersecurity architecture;

1. West African countries can improve their cybersecurity architecture by developing a comprehensive national cybersecurity strategy in each West African countries (He noted this approach has been enforced in Cote divoire). This strategies will address the unique cybersecurity challenges facing each country. The strategy should include combating cybercrime, building capacity, includes measures to protect critical infrastructure.
2. Mr. Laicana recommended that each West Africa countries should establish a dedicated national cybersecurity agency. This agency will be responsible for coordinating and implementing national cybersecurity strategy, also the agency should work closely with private sector and international partners.
3. West African countries can improve their cybersecurity architecture by Increasing awareness to strengthen West Africa infrastructure. West Africa countries can increase cybersecurity awareness among key stakeholders through campaign on safe and online practice, training programmes for government and private employees.

Panel Session

What are the main gaps between the competencies companies seek and those that graduates possess upon completion of cybersecurity-oriented vocational or tertiary studies, what are the remedies to ensure graduates' relevance.

Abdul Hakeem noted keys issues from reading of report presented by Dr. Jimson Olufuye, he highlighted key issues; which are Insufficient resources across the continent, Insufficient legal framework, Relative low awareness, Insufficient cross border cooperation and collaboration.

Way forward from UNECA perspective

- ✓ Strengthening the legal frameworks
- ✓ Enhancing and institutional mechanism regional cooperation
- ✓ Capacity building and Awareness.

He appreciated UNECA initiatives for providing such guidance for west African countries as they work to strengthen their cybersecurity capacity.

On what competencies do organizations need. Alhaji Ajijola responded that the Industries needs a resources person with practical experience.

1. Hence, provided remedy by integrating internships and mentor-ships in the cybersecurity curriculum.
2. Engaging student in practical project in case studies so as to enhance their experience.
3. Up to date knowledge (remedy) regularly updating the curriculum to reflect industries trends.
4. Incorporate input from industries professionals because the cutting edge keeps moving proactively.
5. Encourage ongoing professional development within the faculty

members in making sure student are learning the most relevant materials.

6. The need for specialized skills (specialized tracks) such as the areas of cyber diplomacy, cybercrimes. Also, providing cybersecurity elective courses within cybersecurity programmes that allows students to develop expertise in specific areas of interest.
7. Top skills development into cybersecurity programmes such as collaboration, group project, presentation. collaboration exercise that can help graduate more rounded professionals.
8. Industries certifications: (Remedy) Integrating certification preparation into main stream academics programs within the context of the same academic course. Making students obtained industries recognized credentials. Ensuring the relevant of graduate in the cybersecurity job market.
9. Educational institutions, government, civil society, the media and private sectors needs to collaborate in closing the gaps.

He noted that these can be achieved through; Curriculum reviews, Public-Private Partnership, Promoting the culture of continuous learning and Professional development.

Panel Session

Give an assessment of what has worked and what should be done better in terms of Cybersecurity preparedness in West Africa.

Many West Africa Countries have developed and implemented national cybsecurity strategies to help guide their efforts and better protect their digital assets. These strategies outline the roles and responsibilities of the stakeholders by identifying key risks and measures to mitigate the risk. Ghana for instance has put in place a national cybersecurity policy and strategies which enables it to identify its risks.

Collaboration has increased among West Africa Countries as well as International partners which has led to the sharing of information and best practice on cybersecurity. As a result of collaboration, it has led to the establishment of cybersecurity organization such as ECOWA cybersecurity regional agencies and AU. ECOWAS and AU has also put in place capacity programmes to promote cybersecurity cooperation.

- Establishment of cybersecurity academic by African Union, AU is providing training and education across the continent.
- Policy development is ongoing in the region. National policy has been developed. The policy examines the responsilities of different stakeholders and and establishes measures to mitigate the rising risks.
- Increased awareness should be facilitated across West African nations
- Increasing Public - Private Partnership to promote cybersecurity in West Africa. it has also led to the platform on sharing of expertise and information also development of new cybersecurity solutions.

What should Africa as a whole do to reap from the benefit of creating and innovating its own solutions and technology to counter cyber-attacks??

Seven (6) recommendations were noted by Abdul Hakeem Ajijola on how Africa as a whole can reap from the benefit of creating and innovating its own solutions and technology to counter cyber-attacks.

1. Investing in education and capacity building 2. Supporting of local start up companies 3. Strengthening regional collaboration 4. Promoting private-public partnership 5. Developing a robust legal framework 6.Fostering cross cultural cybersecurity

Panel Session

- In order to ensure there is inclusivity and prosperity in the region, online safety of all citizens must be of high priority including that of the the elders. What special measures and applications could be developed to protect the elders in cyberspace?

Mr. Eric Kouam responded that the first thing to do is the regulation of the utilization of digital tools across the public administration. Basic practice on the usage of digital tool in the public administration should be encouraged.
Awareness also is key, the way technology is going there is need for a control. In terms of control, government can put in place education programme for people to be aware on what to use and tools to use and how to use them.

In Ghana, number of cyber attacks from 2011-2021 was 345,035,390. What measures must be put in place to avoid skyrocketed figures of cyber attacks in the next decade?

On the question of special measures and applications to protect the elderly in cyberspace, Mr. Raymond responded that one of the strategy to be deployed is User friendliness as elderly are not able to use the strict applications like the youth. Without user friendliness there is no inclusivity.

On measures to be put in place to avoid skyrocketed figures of cyber attacks in the next decades, it was recommended that the clarion call is to make cybersecurity training from elementary to tertiary institutions very paramount, in that it should be made one of the courses in tertiary institutions but must be compulsory at all stages of Education across Africa.

Q & A Session from the participants?

- **What are the parameters to ensure Cyber diplomacy?**
- **As Africa, looking at cybersecurity, the applications and systems that we use determine how vulnerable we are. At what point are we considering capability systems designed by Africa engineers to deal with Africa solutions so that security phishers are known?**

Amb. Segun Olugbile emphasized that the best way to get engage in cyber diplomacy is to start with Internet governance. He stressed that Internet governance, IG provides a platform for knowledge sharing, where an individual can have access to various programmes, activities and as well learn the process of Internet governance, those behind it and the role individual can play. This engagement can also spur to cyber diplomacy at the international level and national level.

Alhaji Ajijola emphasized on the importance of Cyber diplomacy. Hence, noted that Africa needs a generation of cyber diplomat. He noted that there are ongoing discussions of the UN which has produced eleven (11) norms on soft laws. Africa's voice needs to be heard. In terms of Africa security solutions, Alhaji Ajijola maintained that there is need for Africa security by design which borne down to innovation, because many Africans are extremely innovative. Hence, recommended that we have to make up practical application of the result in research and development in the African context. In terms of Policy and framework, he noted that Africa Cybersecurity expert group are in the process of developing an African wide cybersecurity strategy which is a work in progress.

- **Considering the technicality involved in cybersecurity, what are the prospect for those who are non science expert or enthusiasts?**

Dr. Jimson Olufuye responded that the key thing needed to get engaged in cyberspace is passion i.e having passion in the Internet processes can help to be rooted in the knowledge. Then one can commeneced from elementary level and scale high. In terms of getting the skills, Dr. Jimson accorded a number of institutions that provide degree in cybersecurity both at the Diploma up to Postgraduate level among them is; National open university in Nigeria etc.

Mr. Ajijola added that for an Art-Class background professional to get into cyber, the passion is foundational. He made reference to his own experience that one of the best cyber professional has had mathematics, history and philosophy.

- **How to get more home grown solutions?**

Dr. Jimson Olufuye responded that **o**rganisations needs to engage African expertise just like United Nations Economic commission for Africa,UNECA is engaging local expertise on the research, emphasized that more of that should be explored.

- **What is the institution doing in Integrating the practical aspect of cybersecurity?**

Dr. Jimson Olufuye responded that there are some practical policies that can be use as a guide. He referenced that UNECA has a model law on cybersecurity, as part of this effort, he recommended that Africa’s need to invest more on cybersecurity. He places emphasis on offline and online security. Because, offline security is very important, if there is no security offline there can’t be economic progress. Same for the online security because a lot of activities have moved online just as been noted by United Nations - UN that whatever applies offline also happens online. Recommended that decision makers should focus more on offline security and investing in research and development should be leverage on.

Closing remarks

Mr Thabo Mashegoane, Chairman AfICTA, thanked everyone on the webinar, and commended the organizing team for conveying the very rich discussions, he commended the insights around policy, capacity development from the perspective of awareness and professional development for cybersecurity intervention. The Chair also commended the panelists for birthing the call for Afrocentric solution in mitigating cybersecurity challenges in West Africa. He also promised that AfICTA would work on leveraging the expertise of the panellist to accomplish these recommendations.

End of Document