KPMG

GFCE GLOBAL FORUM ON CYBER EXPERTISE

Advancing Cybersecurity with Africa

Study Report

The Global Forum on Cyber Expertise

A Report by KPMG

—

August 2022

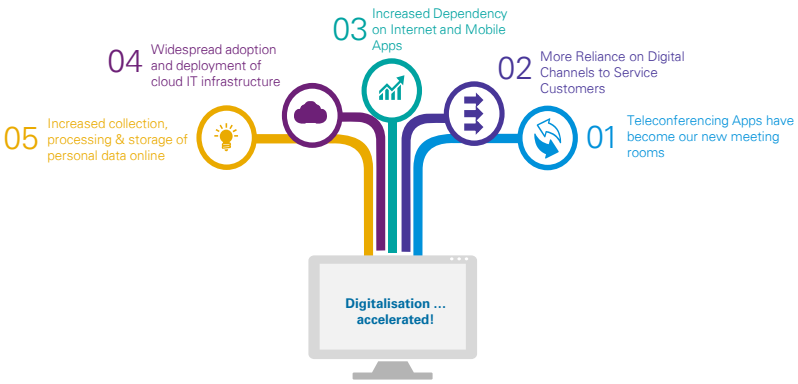
Content

Executive Summary

Executive Summary

Background

Estimated to currently have over 590 million internet users, Africa is digitizing at a rapid scale. Fueled by the Covid19 Pandemic, organizations all over the continent are joining their global counterparts to increase their adoption of digital technologies as a business continuity imperative. The rapid increase in digitization has, however, been faced with attendant challenges.



Notably, there has been the rapid evolution of the threat landscape and emergence of new threats. A recent report by INTERPOL revealed that Africa faces an upsurge in Online Fraud, Digital Extortion, Business Email Compromise, Ransomware, and Botnets. This is in addition to cyber espionage, critical infrastructure sabotage, and other cyber threats causing huge financial losses and threatening the development of the African states. Despite strides by many African states to enhance cyber resilience, the level of commitment to cybersecurity – as well as capacity to respond to threats – remains low compared to other continents.

To help address the gaps, the GFCE has partnered with the African Union to develop cyber capacity to enable AU member states to better understand their current cyber capacities and to support the African nations in strengthening their cyber resilience. This study was carried out by KPMG Nigeria on behalf of GFCE as part of the AU-GFCE collaboration with the aim of presenting the current state of cyber capacities and gaps in Africa from the perspective of the five African regions and developing an agenda with the needs and priorities for the overall continent as well as the five specific regions.

Approach and Methodology

Data for the study was gathered through desk research, workshop, interviews and survey, leveraging GFCE coordination efforts and relationships to reach stakeholders. This was combined with in-house knowledge within KPMG and GFCE networks.

Assessment and Scoring

An assessment was conducted, and scorecard developed for the African regions across five domains. Based on capacity, the regions were indicated as "Developed", "Developing" or "Underdeveloped"

Maturity Analysis

Cybersecurity capacities and gaps were analyzed and used to present a general overview of the cyber resilience of Africa from a regional perspective

Priorities Presentation

Cyber capacity priorities were presented for Africa as a whole and for each African region in particular

Initiatives Proposition

Cyber capacity building initiatives were proposed to help address the cyber priority needs of Africa

Summary of Key Findings

Regional Cyber Capabilities

S/N	Region	Cybersecurity Policy and Strategy/ Cyber Diplomacy	CERT/CSIRT & CIIP/CNIP	Legislation & Legal framework	Awareness, skills and workforce development	Open Internet and cybersecurity standards
1	Central Africa	0.57	0.28	1.61	0.69	0.42
2	Eastern Africa	1.19	1.29	2.09	1.29	1.98
3	Northern Africa	1.76	1.61	2.59	1.82	2.36
4	Southern Africa	1.04	0.86	2.41	1.16	1.22
5	Western Africa	1.47	1.12	2.67	1.02	1.66

The assessment of cyber capacity and gaps of the African regions across the five assessment domains revealed that Northern Africa is "developing" in all domains, Eastern Africa and Western Africa are each "developing" in two domains, while Central Africa and Southern Africa are each "developing" in one domain.

The assessment further revealed that no African region was fully "developed" in any of the five domains. Aside the "developing" domains, others were "underdeveloped". Though efforts have been made, cyber capacity varies from region to region and significant gaps still exist in each region across the domains. The country assessment further revealed a great deal of variation and gaps in the cybersecurity capacity of the individual countries.

Executive Summary

Summary of Key Findings

High Priority Challenges of Africa

Based on the cyber posture of each region and key concerns of the African Cybersecurity stakeholders, 8 high priority cybersecurity challenges and areas for cyber capacity building opportunities for the African continent as well as the five specific regions were developed to serve as an agenda for African stakeholders.

Recommended Imperatives

To address the high priority challenges, the following recommendations were offered as imperatives for African countries:

01 **Commitment to Cybersecurity Culture and Education**

Cyber security curriculum and accompanying training and awareness activities should be designed for schools, organizational staff, government heads, business leaders, and the general public

02 **Development and Implementation of Robust Cybersecurity Strategy**

Comprehensive cybersecurity strategies should be developed at the national level with clear action plans for implementation

03 **Strategic Coordination and Implementation of National Cybersecurity Programmes**

There should be adequate coordination and implementation mechanism including roles, frameworks and resource allocation with respect to national cybersecurity programmes

04 **Development of Robust Legal Framework for Cybersecurity**

Adequate cybersecurity, cybercrime and data protection laws should be enacted, and training conducted for the judiciary and law enforcement stakeholders to facilitate adoption

05 **Implementation of Intelligence Sharing Framework**

Secure channels should be established for information sharing with clear procedures, responsibilities, and operational terms

06 **Prioritization of Cybersecurity in Leadership**

Cybersecurity roles and functions should be prioritized by national governments and organizational executives during strategic decision-making and resource allocation

07 **Prioritization of Commitment to Global Cyber Activities and Cyber Diplomacy**

Cyber diplomats with requisite skills and trainings should be appointed to represent nations at global forums and committees. There is the need for capacity building in the area of cyber diplomacy

08 **Implementation of Secure Procurement Framework and Encouragement of Local Technology Development**

Standards should be developed and implemented for auditing technology solution vendors while support should be given to building local production capacity from ground up

Specific initiatives were further proposed for implementation of the recommendations.

Background

Background

Evolving Digital Landscape in Africa

With a population of over 1.3 Billion people [1] and over 590 million internet users, Africa is fast undergoing a digital transformation. Africa recorded a significant 12,975% growth in internet usage between 2000 and 2021 [2]. Specifically, by December 2020, the internet penetration in the continent stood at 43% [2], led by Kenya, Libya, and Nigeria who had 85.2%, 84.2% and 73% internet penetration, respectively.

In addition to the growing online community, there has been a steady increase in ICT related spending in the continent. A 2018 survey on the funds expended by 48 African countries in the area of ICT showed an 85% increase compared to the previous year [3]. This change in digital trends in the region has further been fueled by the COVID-19 pandemic which stirred the global emergence of several innovative digital technologies and their widespread adoption. It is reported that 25% of the firms in sub-Saharan Africa accelerated the use of digital technologies and increased investments in digital solutions in response to COVID-19 [4].

Overtime, Africa has made significant progress in technological innovation. Though hosting just 0.02% of the global start-up ecosystem valued at 3.8 trillion dollars [5], with the many technological innovations birthing out of the continent such as M-Pesa in Kenya, Interswitch, Flutterwave, and Opay in Nigeria, Go1 and Jumo in South Africa, Fawry in Egypt, among many others, Africa continues to play a leading role in digital financial services deployment [6] and is believed to have the potential of becoming a tech start-up giant.

Evolving Threat Landscape

The upward trend in digitization witnessed across Africa has, however, not been without attendant challenges. The African cyber threat landscape has widened considerably over the years, with attackers constantly evolving their strategies to exploit newer vulnerabilities accompanying the technological evolution.

As recently exposed by INTERPOL, the continent has been plagued by an upsurge in Online Fraud, Digital Extortion, Business Email Compromise, Ransomware, Botnets, among other cyber threats [7]. With South Africa ranking the 3rd most targeted country by Ransomware [8], African organizations saw the greatest increase in ransomware attacks from January to April 2021, at 34%. In addition, a report by Kaspersky indicated that, over 14,071 of the 206,000 mobile malwares detected and blocked by the company for the Middle East, Turkey and Africa between January and June 2021 originated from Nigeria [9] which is Africa's biggest economy.

Furthermore, there are, on average, 3,900 victims of botnets discovered in Africa monthly, and many high-profile instances of Distributed Denial of Service (DDoS) attacks on critical infrastructure have occurred in Africa in the past five years [7]. For example, the 2016 Mirai botnet DDoS attack on Liberia crippled the internet infrastructure of the entire country [10]; and, more recently, in September 2019, a large South African Internet Service Provider (ISP) was knocked offline for an entire day [11].

These are just but few examples of the intense, vast and dynamic nature of African threat landscape. Considering the huge technology dependency of the post COVID-19 world, these trends are expected to remain on the increase as more technologies are rolled out to support Africa's growing economy.

[1] https://www.worldometers.info/world-population/africa-population/

[2] https://internetworldstats.com/stats1.htm

[3] https://www.icafrica.org/en/topics-programmes/spending-by-african-governments-on-infrastructure/

[4] https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AFR.01-2021-PDF-E.pdf

[5] https://nairametrics.com/2021/10/07/africas-startup-ecosystem-is-worth-6-6-billion-gser/

[6] https://www.prweb.com/releases/africa_leads_world_in_digital_financial_services_deployments_with_prepaid_cards_an_important_part_of_mix_says_axiom_prepaid_holdings_reps/prweb17214821.htm

[7] https://cybersecurityworldconference.com/2021/10/30/reading-interpol-the-african-cyberthreat-assessment-report-2021/

[8] https://www.itnewsafrica.com/2021/04/south-africa-ranked-as-3rd-most-targeted-country-by-ransomware

[9] https://punchng.com/nigeria-urged-to-invest-in-cybersecurity-against-spate-of-attacks/

[10] https://www.techrepublic.com/article/how-the-mirai-botnet-almost-took-down-an-entire-country-and-what-your-business-can-learn/

[11] https://mybroadband.co.za/news/internet/324480-south-african-isps-are-under-attack.html

Background

The Need for Cyber Capacity Commitment

In addition to a plethora of other consequences such as confidential information disclosure to public domain, reputational damage and permanent data loss, the unrelenting bombardment of attacks by threat actors has caused member states of the continent huge financial losses. A 2017 report by Kenyan cybersecurity firm, Serianu, pegged the cost of cybercrime in Africa at 3.5 billion dollars, with Nigeria losing 649 million dollars, followed by Kenya who lost 210 million dollars [1]. Another report by UK based cybersecurity company Sophos on "The state of Ransomware 2021" noted that the average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. in an organization in 2021 was 1.85 million dollars [2].

Although there have been considerable strides taken by many AU member states to enhance cybersecurity postures, Africa's levels of commitment to cybersecurity – as well as capacity to respond to threats – remains low compared to other continents. African businesses and banking systems have been described as low hanging fruit for hackers from across the globe; a situation attributed to vulnerable systems and lax cybersecurity practices [3]. As internet penetration rises and systems become more connected, critical infrastructure across Africa will likely become even more vulnerable to costly, disruptive cyberattacks. This, therefore, as a matter of urgency, calls for renewed and more focused commitment in building cyber capacity and combating cybercrime by African states to allow for the safe, secure, and peaceful reaping of the full benefits of technology in Africa.

AU-GFCE Collaboration

The Global Forum on Cyber Expertise (GFCE) is a global multi-stakeholder platform of more than 140 members and partners from all regions of the world aiming to strengthen cyber capacity and expertise globally through the facilitation of international collaboration. The GFCE has partnered with the African Union (AU) to develop cyber capacity to enable AU member states to better understand their current cyber capacities and to support the African nations in strengthening their cyber resilience.

As part of the AU-GFCE collaboration, this study was carried out by KPMG Nigeria on behalf of GFCE. This study is aimed at presenting the current state of cyber capacities and gaps in Africa from the perspective of the five African regions and developing an agenda with the needs and priorities for the overall continent as well as the five specific regions.

KPMG leveraged its resources, tools and knowledge to gather, analyze data and build a case for Africa during the study. Additionally, the AU-GFCE network of official contacts with governments throughout Africa was tapped into at different points to engage stakeholders of various African states and organizations towards the success of the study.

[1] https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[2] https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[3] https://moguldom.com/257909/10-things-to-know-about-cyberattacks-targeting-africa/

Study Approach and Methodology

Approach

Overview of Study Approach

The execution of the study followed a multi-step approach including data acquisition and analysis, validation of findings and reporting. Data from both secondary and primary sources was considered by the project coordination team in executing the study. Desk research was employed in acquiring secondary data while stakeholder workshop, focus group meetings and interviews where possible, were employed to acquire primary data as well as validate secondary data. The data was combined with in-house information already available within KPMG's knowledge repository and those received from surveys already conducted by GFCE to carry out this study. The preparation of the final report followed a multi-stakeholder review process. Below is an overview of the steps followed in executing the study:

Plan

- The study execution was coordinated by a KPMG project team working jointly with key GFCE and other stakeholders
- Discussions were held and agreements on study timeline and work plan reached by the study execution team with relevant stakeholders
- Key stakeholders were identified, and clear roles and responsibilities established for the project team
- Schedules for interviews and focus group meetings with relevant stakeholders were developed

Project Plan

Research and Analyze

- Data on current cyber capacities within the African region was gathered from relevant sources.
- Gaps regarding cybersecurity and cybercrime needs for the African region was analyzed taking into consideration the national specifics in each state
- Existing GFCE coordination efforts and relationships were leveraged to further acquire data
- Collected data was used to analyze and present the cyber capacity and gaps of Africa and specifically the African regions

Preliminary Findings

Workshop and Interview

- An in-person workshop with representatives from key African stakeholders and African countries was held at The Hague, Netherlands to gain input from stakeholders on the cybersecurity challenges/ needs of Africa
- Virtual (follow-up) interviews were conducted with selected representatives to validate preliminary findings on the regional and national cyber capacities
- Focus group meetings with representatives from key regional organizations and African countries were facilitated where possible, to further gain perspective and validate preliminary findings

Further Findings

Report

- Combining findings from the stakeholders' workshop, gaps analysis, interviews and country survey by GFCE, priority areas for cyber capacity building opportunities for the African continent as well as the five specific regions were developed to serve as an agenda for African stakeholders
- Draft report on the current state of cyber capacities and gaps in Africa from the perspective of the five African regions was developed and presented to key stakeholders
- Feedback from stakeholders on the draft report was taken into consideration in the preparation of the final report

Study Report

Analysis Work-Flow

The following steps were taken to analyze cyber capacities and gaps and present priorities for Africa and the five African regions:

Assessment and Scoring

Using acquired data, an assessment was conducted, and scorecard developed for the African countries as well as the five African regions based on a **methodology** specifically developed for the assessment

Maturity Analysis

Specific cybersecurity capacities and gaps were considered on a country-by-country basis, and this was used to present a general overview of the cyber resilience of Africa from a regional perspective

Priorities Presentation

Cyber capacity priorities were presented for Africa as a whole, and for each African region based on the cyber posture of each region and based on the key concerns of the African Cyber stakeholders

Initiatives Proposition

Cyber capacity building initiatives were proposed to help address the cyber priority needs of the African regions, bridge the gap in cyber capacity and further advance cyber resilience in the African region

Assessment Methodology

Overview of Methodology for Cyber Capacity Assessment

Assessment Domains

This study considered five domains in the assessment of the cyber capacity and gaps of the AU member states. These domains which were developed by GFCE and mapped with the five GFCE working groups in alignment with the Delhi communique, [1] are as follows:

- **Cybersecurity Policy and Strategy/ Cyber Diplomacy** which measures the level of development and implementation of cybersecurity policies and strategies across each region.
- **CERTS/CSIRT and CIIP/CNIP** which measures the capacity and readiness of states in the African regions to protect their critical national infrastructure and respond to computer security incidents and emergencies.
- **Legislation and Legal Framework** which measures the development and implementation of laws and regulations by governments of the various countries in each of the African regions to adequately address cybersecurity and cybercrime, and the level of commitment to this per region.
- **Awareness, Skills and Workforce Development** which measures the level of efforts towards cybersecurity education, awareness, cultural development and human capacity development by each country and across each African region.
- **Open Internet and Cybersecurity Standards** which measures the adoption and implementation of information security standards, guidelines and best practices by each of the countries and across each region.

Assessment Steps

Data from two sources, the Global Cybersecurity Index (GCI) 2020 [2] and National Cyber Security Index (NCSI) retrieved January 2022 [3], was considered in developing indicators for assessing the AU member states and the various African regions. A four-step process was adopted to complete the assessment as follows:

- **Step 1**: Each of the five focus domains was mapped to corresponding segments of each data source to develop indicators for assessing each country per domain. Data source segments comprised of one or more scored factors. Details of the domain to data source mapping is given in the Appendix.
- **Step 2**: For each domain, the contributing scores were averaged per data source to produce the source rating. Source ratings for all data sources were normalized to a common scale of 0 to 5.
- **Step 3**: Each country was scored on the 5 domains against a scale of 0 to 5 by averaging the normalized source ratings. Where data was only available for a country in a specific domain from one data source, the normalized source rating was taken as the country score. Regions were scored per domain by averaging the scores of all countries in that region for that domain.
- **Step 4**: For each domain, scores were used to indicate regions as either **"underdeveloped"**, **"developing"** or **"developed"** in terms of cyber capacity. The indicators were represented in a color-coded systems to give a general overview of the cyber capacity and gaps in Africa on regional basis as given below:

Developed	>3.5
Developing	1.5>3.5
Underdeveloped	<1.5

Limitations

The following limitations were identified during this study:

- During the assessment process, there was no available data from some data sources for certain countries. The scoring may, therefore, not give a true representation of the cyber capacity of some countries relative to others in certain assessment domains as some countries were scored using data from one source and others scored using data from the two sources.
- Another limitation is the difference in the time within which each data source was published or last updated.
- The assessment also inherits whatever shortcomings that may be inherent in the development of the data sources from the original research.

The authors recognize that the methodology developed in this study report is not the definitive method of measuring the level of growth and needs in cyber security in Africa. Assessment such as the "Cyber Readiness Index (CRI) by the Potomac Institute for Policy Studies (PIPS) and the Cybersecurity Capacity Maturity Model for Nations (CMM) by the Global Cyber Security Capacity Centre (GCSCC), University of Oxford, and partners, are also available. They can be found in greater detail through the GFCE Global Overview of Assessment Tools (GOAT).

[1] https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

[2] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

[3] https://ncsi.ega.ee/ncsi-index/?order=-ncsi

Overview of Africa's Cyber Capacity

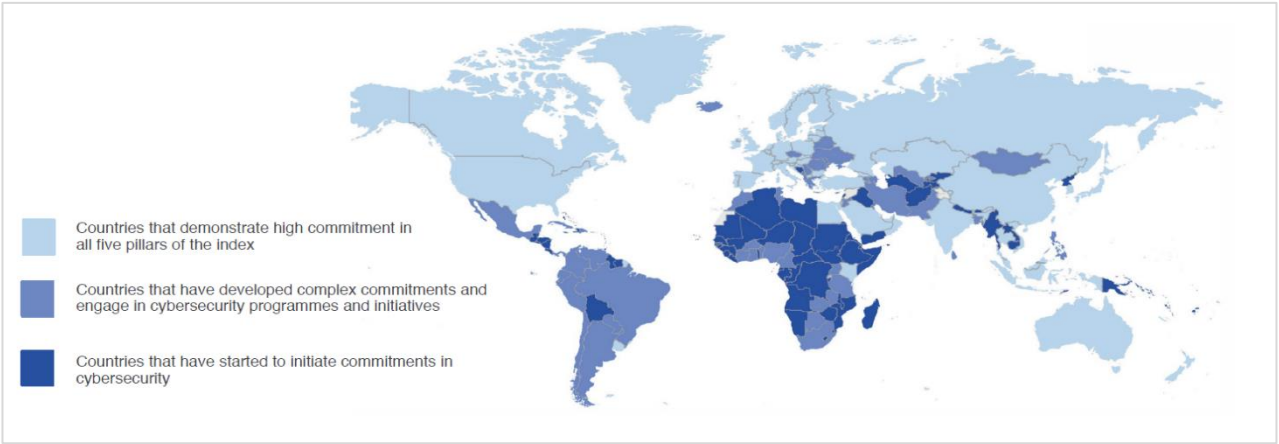
Overview of Africa's Cyber Capacity

General Look on Africa's Cyber Capacity Compared to Other Continents

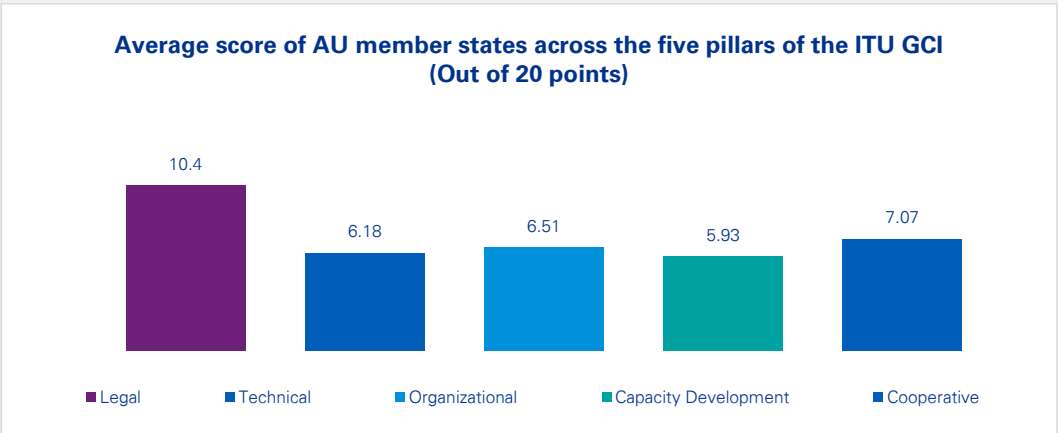
Based on the Global Cybersecurity Index (GCI) 2020 published by the International Telecommunications Union (ITU) [1], Africa has the highest concentration of countries that are just starting to initiate commitments to cybersecurity. This is as opposed to other regions like Europe who have a high fraction of countries at established cyber maturity stages.

In the overall country ranking by the GCI which placed countries from position 1 to 182 based on cyber capacity, 21 AU member states made it to the list of top 100 countries, 7 AU member states made it to the top 50 ranked countries, 2 AU member states made it to the top 30 list while only 1 African country was among the top 20 countries.

Presented in the figure below is a representation of the level of cybersecurity commitment of countries globally based on the ITU GCI (2020):



The ITU GCI defines five pillars for measuring cybersecurity posture namely: **Legal Measures, Technical Measures, Organizational Measures, Capacity Development Measures and Cooperation Measures.** Under the legal measures, for example, only about 33% of AU member states scored up to 15 out of 20 points while about 85% of European states scored higher than 15 points. On the organizational measures, 29% of AU member states scored above 10 points compared to Americas, Europe and Asia-Pacific where 26.3%, 87% and 47.4% of the countries respectively scored above 10 points. Review of the capacity development measures showed that 29% of AU member states scored higher than 10 points while 23.7%, 84.8% and 42.1% of Americas, Europe and Asia-Pacific respectively scored higher than 10 points.

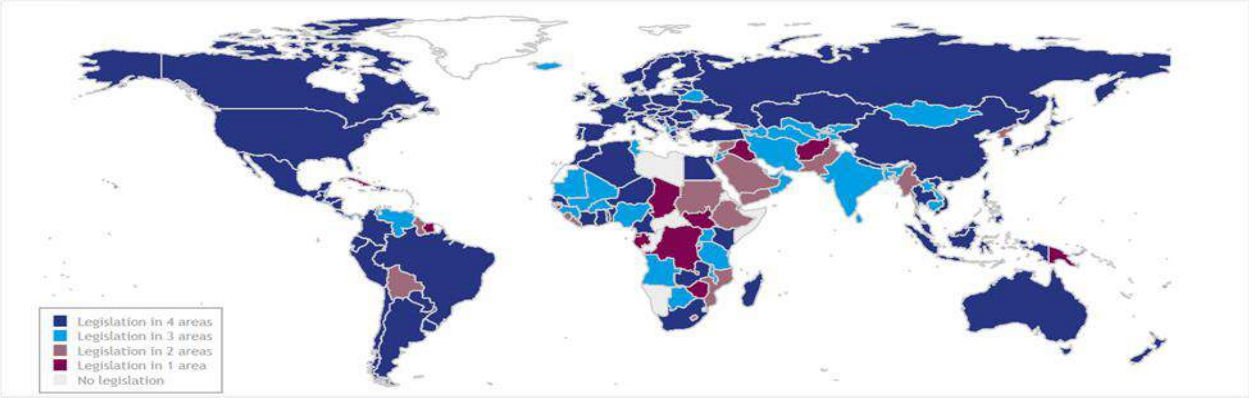


[1] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

Overview of Africa's Cyber Capacity

General Look on Africa's Cyber Capacity Compared to Other Continents

The cyber law tracker by the United Nations Conference on Trade and Development (UNCTAD) [1] as of February 2022 showed that in the four cyber law areas defined by the organization namely: e-transaction, consumer protection, data protection/ privacy, and cybercrime, Africa had the lowest percentage of countries with full cyber legislation compared to other regions. While cyber legislation had been fully adopted in all four areas by majority of countries in other regions, the level of cyber legislation adoption varied considerably among African countries as shown below:



Source: UNCTAD

Furthermore, from the National Cyber Security Index (NCSI) ranking by E-Government Academy, Estonia [2], retrieved January 2022, no African country was among the top 40. Egypt and Zambia narrowly made it to the top 50 ranked countries at positions 48 and 49 respectively.

On the area of international cooperation for incident and emergency response, the membership list of Forum of Incident Response and Security Teams (FIRST) [3] as of January 2022 showed the least level of participation from Africa. Out of the 608 FIRST member teams, 23 teams (i.e., less than 4%) were from African countries. Furthermore, out of 55 African countries, 15 were represented in FIRST as some countries were represented by more than one incident response team.

Global FIRST membership distribution as of January 2022 is represented below:

Source: FIRST

A look into global activities on cyber diplomacy reveals limited participation by African countries on cyber norms development. An example of this is the membership of the 4 United Nations Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security- formerly on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE on Cybersecurity)- that produced a consensus report[4]. Out of 25 members of the 2019/21GGE, only 4 were African countries. Similarly, out of 20 members of the 2014/15 GGE, only 3 were African countries, and out of 15 members each of the 2009/10 and 2012/2013 GGE, there was only 1 African country in each case.

Put together, these factors further validate the assertion that Africa's levels of commitment to cybersecurity – as well as capacity to respond to threats – remains low compared to other continents.

[1] https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide

[2] https://ncsi.ega.ee/ncsi-index/?order=-ncsi

[3] https://www.first.org/members/map

[4] https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

Regional Cyber Capabilities

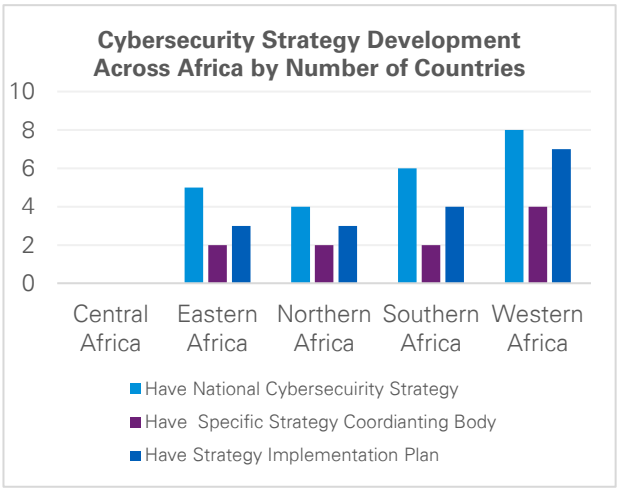
Regional Cyber Capabilities

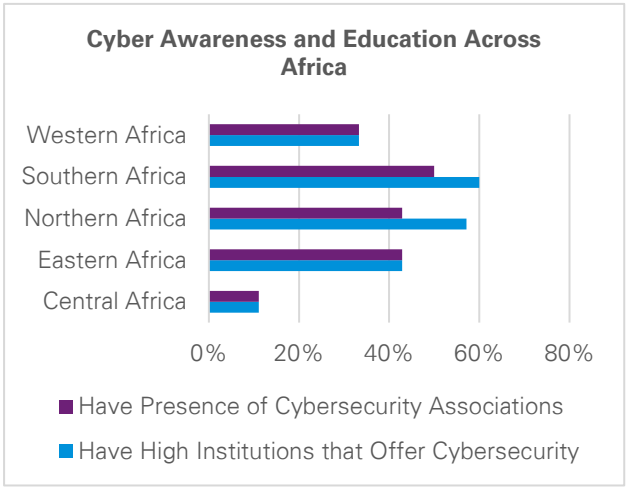
Assessment of Africa's Cyber Capacity Based on Regions

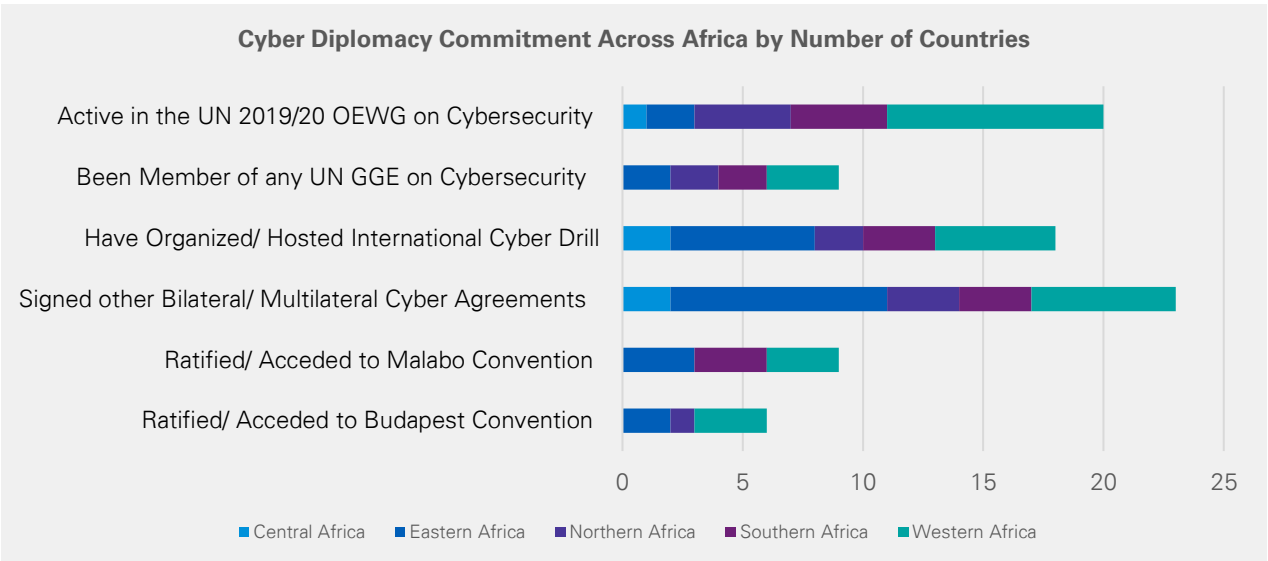
Regional Scorecard

S/N	Region	Cybersecurity Policy and Strategy/ Cyber Diplomacy	CERT/CSIRT & CIIP/CNIP	Legislation & Legal framework	Awareness, skills and workforce development	Open Internet and cybersecurity standards
1	Central Africa	0.57	0.28	1.61	0.69	0.42
2	Eastern Africa	1.19	1.29	2.09	1.29	1.98
3	Northern Africa	1.76	1.61	2.59	1.82	2.36
4	Southern Africa	1.04	0.86	2.41	1.16	1.22
5	Western Africa	1.47	1.12	2.67	1.02	1.66

Overview of Regional Cyber Posture

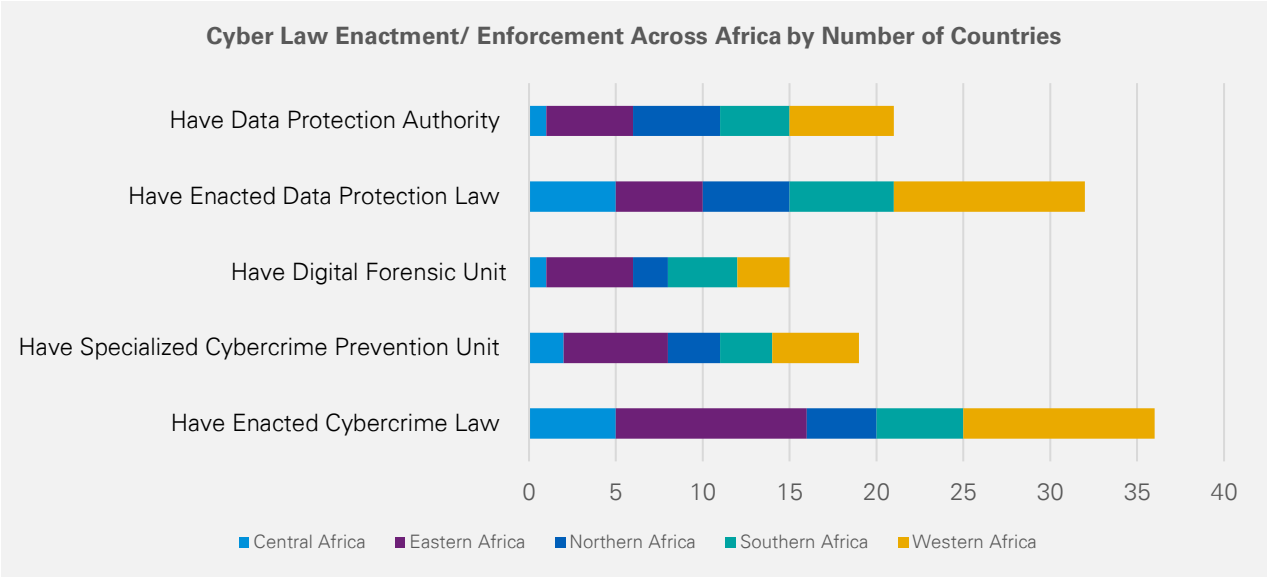


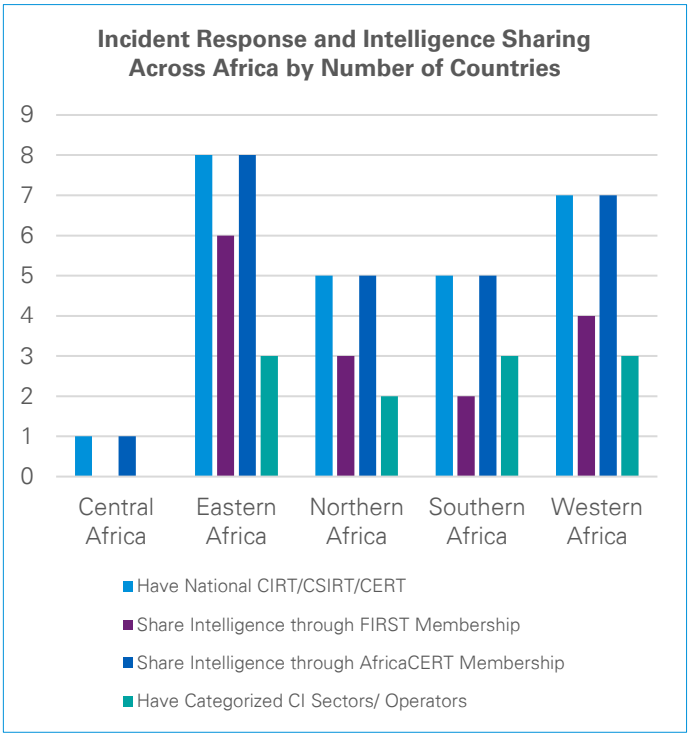


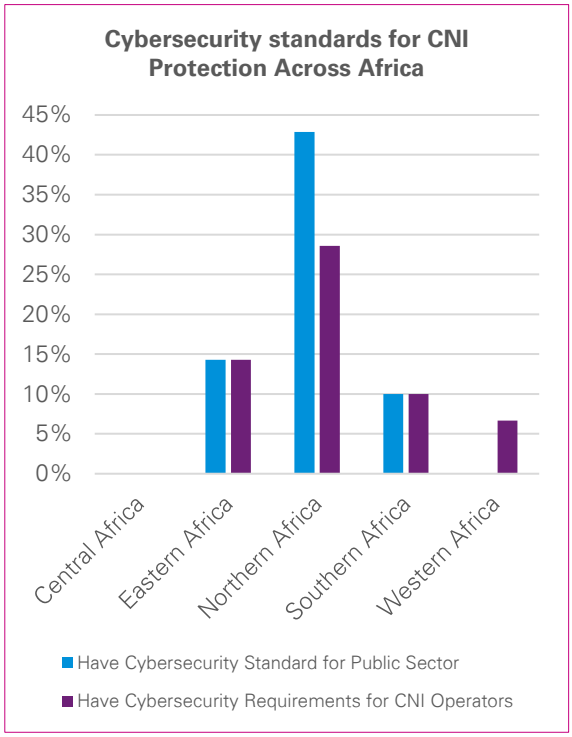


Regional Cyber Capabilities

Overview of Regional Cyber Posture







Regional Cyber Capabilities

Key Insights on the Regional Cyber Posture

Region	Capacity	Gap
CENTRAL AFRICA	• 2 countries in the region have so far either hosted or co-organized a regional/ international cyber drill • The existing incident response team in the region is a member of AfricaCERT • More than half of the countries in the region have a cybercrime law • Over 50% of the Central African countries have a data protection law	• No country is known to have a national cybersecurity strategy • None of the states has ratified/ acceded to the Budapest convention • None of the states has ratified/ acceded to the Malabo convention • No country represented the region in any of the convened UN GGE on Cybersecurity • One of the states actively participated in the UN 2019/2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (UN OEWG on Cybersecurity) • About 22% of the Central African states are known to have signed bilateral/ multilateral cybersecurity agreements with other nations • 1 out of 9 countries has a national incident response team • No country in the region is represented in FIRST • No country in the region is known to have identified/ categorized its critical infrastructure sectors/ operators • Majority of the countries that have a cybercrime law have no specialized cybercrime prevention unit • One country in the region is known to have a specialized forensic investigation unit • One of the countries is known to have a data protection authority • One Central African country is known to have high institutions that offer cybersecurity education/ training at Bachelors/ Masters level • One countries in the region is known to have the presence of a cybersecurity association • No country in the region is known to have developed/ adopted cybersecurity standards for the public sector • No country in the region is known to have set cybersecurity requirements for CNI sector operators
EASTERN AFRICA	• Majority of the countries that have a cybersecurity strategy also have an action plan for strategy implementation • About 6 countries in the region- which so far is highest in Africa- have either hosted or co-organized a regional/ international cyber drill • 2 countries have represented the region each in at least one of the convened UN GGE on Cybersecurity • More than 60% of the states have signed bilateral/ multilateral cybersecurity agreements with other nations aside the Budapest and Malabo conventions • More than 50% of countries in the region have a national incident response team • 6 out of 8 national incident response teams in the region are FIRST members, enabling cooperation • All national incident response teams in the region are AfricaCERT members • About 78% of countries in the region have a cybercrime law • More than half of the countries who have a cybercrime law also have a specialized cybercrime prevention unit • All countries who have a data protection law also have a data protection authority	• About 35% of the countries have a national cybersecurity strategy • Most countries who have a national cybersecurity strategy have no coordinating body specifically tasked with implementing the strategy • 2 out of 14 countries in the region have ratified/ acceded to the Budapest convention • 3 out of 14 countries in the region have ratified/ acceded to the Malabo convention • Two Eastern African countries actively participated in the activities of the UN 2019/2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security • Majority of countries in the region are yet to categorize their critical infrastructure sectors/ operators • Only a little above one-third of the states have a data protection law • Most of the countries have no specialized forensic investigation unit • Less than half of countries in the region have institutions of higher learning that offer cybersecurity education/ training at different levels • Less than half of the states in the region have the presence of a cybersecurity association • Two countries in the region are known to have developed/ adopted cybersecurity standards for the public sector • About 14% of countries in the region are known to have set cybersecurity requirements for CNI sector operators • 3 of the top 6 countries with the highest phishing attempts in Africa- from the 2021 INTERPOL most prominent cyber attacks in Africa- were Eastern African countries • Eastern African countries made it to the list of the top 6 most affected countries in 4 out of 5 cyber threats most prevalent in Africa from the 2021 INTERPOL most prominent cyber attacks in Africa

Regional Cyber Capabilities

Key Insights on the Regional Cyber Posture

Region	Capacity	Gap
NORTHERN AFRICA	• About 57% of the countries have developed a national cybersecurity strategy • Three-quarters of the countries that have a national cybersecurity strategy also have an implementation plan • Half of the countries that have a national cybersecurity strategy also have a coordinating body for implementing it • 2 countries in the region have so far either hosted or co-organized a regional/ international cyber drill • About 57% of the countries actively participated in the UN 2019/2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security • 2 countries have represented the region each in at least one of the convened United Nations Group of Governmental Experts on Cybersecurity • About 43% of the Northern African states have signed bilateral/multilateral cybersecurity agreements with other nations aside the Budapest and Malabo conventions • Over 71% of the countries have a national incident response team • About 60% of the national incident response teams are FIRST members • All the national incident response teams are AfricaCERT members • 4 out of 7 countries in the region have a cybercrime law • 75% of the countries that have a cybercrime law also have a specialized cybercrime prevention unit • About 71% of the nations have a data protection law • All the countries who have a data protection law also have a data protection authority • About 57% of the countries have high institutions that offer cybersecurity education/ training at different levels • About 43% of the states in the region have the presence of a cybersecurity association • About 43% of the countries are known to have developed/ adopted cybersecurity standards for the public sector	• 1 out of 7 countries in the region is known to have ratified/ acceded to the Budapest convention • No country has ratified/ acceded to the Malabo convention • Less than 30% of the countries have identified/ categorized their critical infrastructure sectors/operators • Less than one-third of the countries have specialized forensic investigation unit • About 57% of countries in the region are yet to have set cybersecurity requirements for CNI sector operators • 3 of the top 6 countries with the highest number of digital extortion IP senders- from the 2021 INTERPOL most prominent cyber attacks in Africa- were Northern African countries • 3 of the top 6 countries with the highest number of ransomware detections- from the 2021 INTERPOL most prominent cyber attacks in Africa- were Northern African countries • Northern African countries made it to the list of top 6 most affected countries in 4 out of 5 cyber threats most prevalent in Africa from the 2021 INTERPOL most prominent cyber attacks in Africa.
SOUTHERN AFRICA	• 60% of the Southern African countries have a national cybersecurity strategy • Two-thirds of the countries that have a national cybersecurity strategy also have an action plan for strategy implementation • 3 countries in the region have so far either hosted or co-organized a regional/international cyber drill • 2 countries have represented the region each in at least one of the convened United Nations Group of Governmental Experts on Cybersecurity • 50% of the countries have a national incident response team • All the national incident response teams are AfricaCERT members • 50% of the countries have a cybercrime law • 60% of the countries that have a cybercrime law also have a specialized cybercrime prevention unit • 60% of the countries have a data protection legislation • Two-thirds of the countries who have a data protection law also have a data protection authority • At least 60% of the countries have institutions of higher learning that offer cybersecurity education/ training • 50% of the states are known to have the presence of a cybersecurity association	• Most of the countries who have a national cybersecurity strategy have no specific coordinating body tasked with implementing the strategy • None of the countries has ratified/ acceded to the Budapest convention • Three countries have ratified/ acceded to the Malabo convention • Less than half of the states actively participated in the UN 2019/2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security • About 30% of the states have signed bilateral/ multilateral cybersecurity agreements with other nations aside the Budapest and Malabo conventions • About 30% of the countries are known to have identified/ categorized their critical infrastructure sectors/ operators. • 2 of the countries are represented in FIRST • Less than half of the countries are known to have a forensic investigation unit. • Two countries are known to have developed/ adopted cybersecurity standards for the public sector • One country is known to have set cybersecurity requirements for CNI sector operators.

Regional Cyber Capabilities

Key Insights on the Regional Cyber Posture

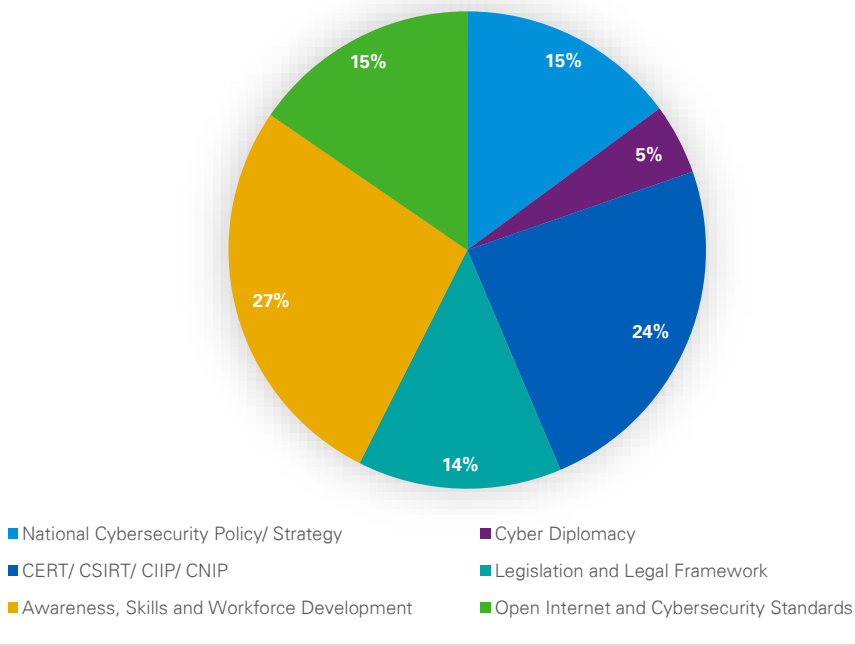
Region	Capacity	Gap
WESTERN AFRICA	• More than half of the countries have a national cybersecurity strategy • About 87% of the countries who have a national cybersecurity strategy also have an action plan for implementing the strategy • Half of the countries who have a national cybersecurity strategy also have a coordinating body specifically tasked with implementing the strategy • About 5 countries have so far either hosted or co-organized a regional/international cyber drill • 9 countries- which was highest from any African region- actively participated in the UN 2019/2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security • 3 Western African countries- which is the highest participation from an African region- have represented the region each in at least one of the convened United Nations Group of Governmental Experts on Cybersecurity • More than half of the Western African national incident response teams are FIRST members • All national incident response teams in the region are AfricaCERT members • Almost three-quarters of the countries have a cybercrime law • All the countries who have a cybercrime law also have a data protection legislation • More than half of countries who have a data protection law also have a data protection authority	• 3 out of 15 countries in the region have ratified/ acceded to the Budapest convention • 3 out of 15 countries in the region have ratified/ acceded to the Malabo convention • About 40% of Western African countries have signed bilateral/ multilateral cybersecurity agreements with other nations aside the Budapest and Malabo conventions • About 46% of the countries have a national incident response team • About 20% of the Western African nations are known to have identified/ categorized their critical national infrastructure • About 3 out of 15 countries have a specialized forensics unit • Less than half of the countries who have a cybercrime law also have a specialized cybercrime prevention unit • Less than 40% of countries in the region have high institutions that offer cybersecurity education/ training at different levels • About 33% of countries in the region are known to have the presence of cybersecurity associations • No country in the region is known to have developed/ adopted cybersecurity standards for the public sector • One country in the region is known to have set cybersecurity requirements for CNI sector operators • 3 of the top 6 countries with the highest number of Business Email Compromise (BEC) actors in Africa- from the 2021 INTERPOL most prominent cyber attacks in Africa- were Western African countries • Western African countries made it to the list of top 6 most affected countries in all 5 categories of cyber threats most prevalent in Africa from the 2021 INTERPOL most prominent cyber attacks in Africa

High Priority Cyber Security Challenges of Africa

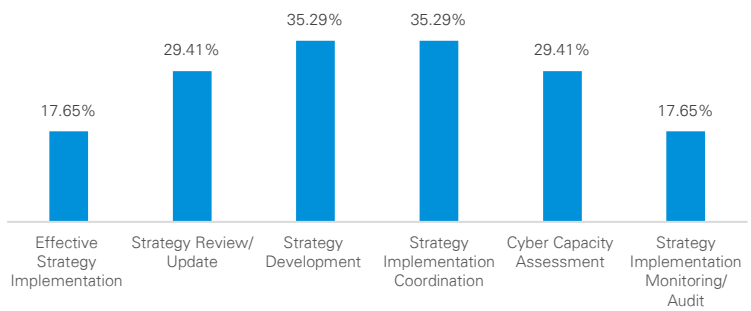
Position of African Stakeholders on Cybersecurity Challenges

The section on Regional Cyber Capabilities shows that while efforts have been made, gaps still exist both at regional and state levels. As would be expected, these gaps continue to pave way for many cybersecurity challenges which are bedeviling the continent. On 23 and 24 November 2021, the GFCE and Africa Cyber Capacity Building Coordination Committee held a workshop on 'CCB in Africa' at The Hague, Netherlands. Over the course of the two days, panelists and representatives from over 20 African nations collaborated on the topic of discussion, exploring cyber capacities, gaps, challenges and priorities for Africa. Among some of the key issues raised by stakeholders were insecure procurement, poor cooperation and intelligence sharing, inadequacy of strategy and ineffective implementation, poor awareness of laws, cyber norms, cyber hygiene practices, etc. These challenges as well as others from analysis were further validated by stakeholders during follow up interviews and in survey responses. Presented below are key insights from the responses of 17 African nations in a survey on CCB Needs conducted by GFCE:

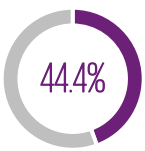
Percentage Share of Each Domain on the CCB Needs Identified by Survey Respondents



Percentage of Countries That Identified the Various CCB Needs Relating to National Cybersecurity Strategy



Of African Nations that outlined Cyber Diplomacy as a CCB Need indicated the Need for Capacity Building on International Cyber Norms

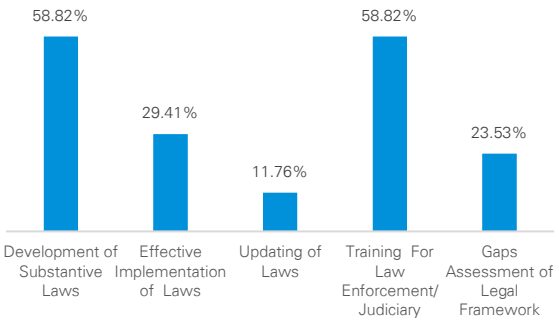


Of African Nations that outlined Cyber Diplomacy as a CCB Need indicated the Need for Capacity Building on Diplomatic Approaches

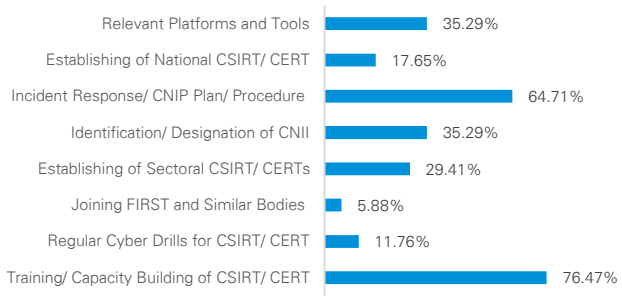
High Priority Cybersecurity Challenges of Africa

Position of African Stakeholders on Cybersecurity Challenges

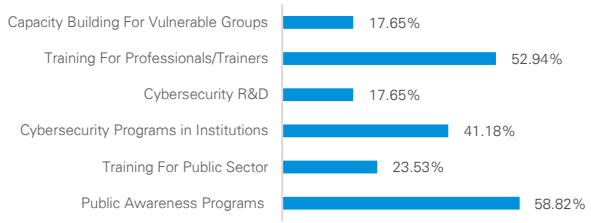
Percentage of Countries That Identified the Various CCB Needs Relating to Legislation and Legal Framework



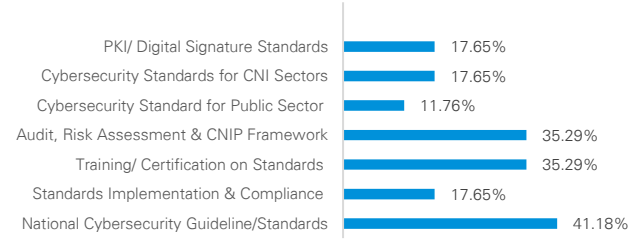
Percentage of Countries That Identified the Various CCB Needs Relating to CERT/ CSIRT/ CIIP/ CNIP



Percentage of Countries That Identified the Various CCB Needs Relating to Awareness, Skills and Workforce Development



Percentage of Countries That Identified the Various CCB Needs Relating to Open Internet & Cybersecurity Standards



Africa's Top 8 Cybersecurity Challenges

1. **Cybersecurity Culture and Education**

2. **Cybersecurity Strategy**

3. **Coordination/ Implementation Mechanism**

4. **Legal Framework**

5. **Cooperation and Intelligence Sharing Framework**

6. **Leadership Commitment and Executive Communication**

7. **Participation in Global Cybersecurity Activities & Cyber Diplomacy**

8. **Secure Procurement and Technology Self-Sufficiency**

High Priority Cybersecurity Challenges of Africa

Africa's Top 8 Cybersecurity Challenges

01 Cybersecurity Culture and Education

Despite the noteworthy strides which have been made by many African nations towards developing cyber capacity, lax cybersecurity practices [1] and poor awareness continue to sabotage efforts. The result is the upsurge in successful cyber attacks across Africa. According to a report by INTERPOL [2], ransomware threat is expanding across the African continent with more than 61% of companies in the region allegedly affected by ransomware in 2020 alone. One other thing to note from the INTERPOL report is that each of the 5 most prominent cyber threats in Africa, in one way or another, leverages phishing and other forms of social engineering which tend to take advantage of human weaknesses rather than technology, or attack techniques which exploit unpatched systems and other low-tech loopholes that could easily be mitigated with the right technical skills and practices. This means that though cyber capacity may appear to exist, human vulnerabilities, made possible by low cyber awareness and poor cultural practices, still opens the stage for successful cyber attacks.

02 Cybersecurity Strategy

The cyber capacity assessment of African countries across all regions shows that 23 out of 54 African countries have developed a national cybersecurity strategy, meaning that more than 50% of the African nations still lack a national cybersecurity strategy. Furthermore, majority of the developed strategies are ineffective in design, implementation and impact, and are not being timely reviewed and updated to meet rapid technological changes. It is estimated that most of the strategies lack minimum required ingredients; namely a threat assessment to identify the scope and scale of the country's cyber threat, a plan of action for addressing the threats, a timeline for implementing the plan, an assignment of responsibilities to key stakeholders for effective implementation, and a provision for allocation of resources for the implementation [3]. This, however, only speaks to the content of the strategy document itself and does not consider other factors for reaching a "developed" stage in cyber capacity.

Nevertheless, a fully inclusive cybersecurity strategy serves as the very foundation for understanding the threat landscape and cybersecurity needs of a nation, designing and implementing solutions and effectively coordinating efforts across government, private-sector, civil society and other stakeholders towards attaining national cybersecurity maturity.

[1] https://moguldom.com/257909/10-things-to-know-about-cyberattacks-targeting-africa/

[2] https://www.interpol.int/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

[3] https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

Africa's Top 8 Cybersecurity Challenges

03 Coordination/ Implementation Mechanism

Policies, strategies, legislations, norms, agreements and other key instruments become effective only when there are strong implementation mechanisms. Same way the police will have no legal grounds to combat cybercrime without a requisite law, a cybercrime legislation will serve no useful purpose where there is no cybercrime police/enforcer, or where the cybercrime police lack basic computer forensic investigation capabilities. This is just one example amongst many to illustrate the importance of well-established implementation mechanisms in driving cyber maturity. One major gap observed in many of the leading African countries in terms of cyber maturity is ineffectiveness in implementation. Most African countries who have a national cybersecurity strategy fail to conduct baseline threat assessment which enables proper monitoring and progress measurement of implementation efforts [1]. Also, it is observed that coordinating bodies, audit/monitoring and control frameworks, clear responsibilities and resources for cyber strategy implementation are missing in many African countries, even when they are contained in the national cybersecurity strategy. In Nigeria, for example, eight years since the publication of the first version of the strategy, the planned National Cybersecurity Coordination Centre for effective monitoring of strategy implementation is yet to be established [2]. Most cybercrime investigation outfits in Africa till date rely on the traditional investigation approach with limited forensic capabilities and only few countries have trained judges specially in cybercrime adjudication.

04 Legal Framework

The rate of cybercrime continues to rise globally, and Africa is not exempted. Cybercrime is estimated to cost Africa over 4 billion US dollars annually [3]. One major reason why cybercrime thrives in Africa is unavailability of laws that adequately address cybercrime. The cyber capacity assessment of the countries across all regions shows that one-fourth of African countries have attained the "developed" stage in the Legislation and Legal Framework domain. Cybersecurity legislation is currently inexistent in many African countries, and for some countries, existing cybersecurity laws have been viewed as ambiguous, broad and limited in applicability.

In Democratic Republic of Congo, for example, it is difficult to legally prosecute cybercrime due to lack of requisite cybercrime law [4]. Also, Sub-Saharan Africa has been labelled a new cybercrime harbor partly due to weak cybercrime laws [5]. Furthermore, while the assessment shows that 32 African countries have each enacted a data protection law, active data protection laws are reported to be present in less than 20% of African countries [3]. Also, inability to implement effective cyber regulations, such as regulations on social media usage, forces many African countries to take alternative measures which have far reaching effects on the economy. For instance, countries like Chad, Cameroon, Algeria and Ethiopia have been reported to totally shutdown the internet in a bid to regulate social media usage during election, disrupting communications between the country residents and the outside world [3]. Similarly, Nigeria, Africa's largest economy, completely placed a ban on the usage of Twitter in June 2021 [6]; this government action lasted for more than 6 months, creating difficulties for many small-scale businesses that depended on the platform to reach target markets.

[1] https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

[2] https://www.thecable.ng/policy-undress-builds-on-dasukis-brainchild-7-things-you-need-to-know-about-buharis-cybersecurity-policy

[3] https://www.itnewsafrica.com/2020/10/the-state-of-cybersecurity-in-africa/

[4] https://capsud.net/2020/05/20/rdc-la-justice-impuissante-face-a-la-cybercriminalite/

[5] https://www.openaccessgovernment.org/africas-cybersecurity-problems-impact-us-all/81354/

[6] https://guardian.ng/news/nigeria-announces-twitter-ban-on-twitter/

Africa's Top 8 Cybersecurity Challenges

05 Cooperation and Intelligence Sharing Framework

The cyber capacity assessment across the entire African region clearly shows that some countries are far more cyber mature than others. While some nations have recorded great achievements in implementing a well coordinated incident reporting and response process, for example, others still struggle with categorizing incidents. Stakeholders during the workshop at the Hague deliberated on the issue of maintaining an intelligence sharing framework. Lack of appropriate intelligence sharing framework between countries is partly responsible for the huge cyber maturity gap observed in different member states. At the national level, this also explains the difference in cyber capacity between government and private players and between government organizations, as the entities work within the confines of their knowledge base.

06 Leadership Commitment and Executive Communication

Another challenge paving way for cyber threats across Africa is the poor leadership commitment and executive communication present in many government and private entities in the region. This challenge was also highlighted by African stakeholders during the workshop at the Hague. Africa, for example, faces a growing array of cyber threats, yet most African countries still lack a comprehensive national cybersecurity strategy. Poor understanding of potential business impacts of cyber attack by business executives also accounts for this challenge. While most business leaders would agree that cybersecurity is a top priority, they have a plethora of other top priorities, such as financial pressures and digital transformation initiatives to deal with [1], and for some, cybersecurity is usually an afterthought when making big strategic decisions [2]. Even when an organizational workforce possesses the requisite cyber awareness, skills and competencies, lack of leadership commitment to cybersecurity expressed through appropriate actions including executive communication poses a challenge to good cybersecurity practices within the organization, thus exposing the organization to cyber threats. A typical example of poor leadership commitment is the theft of an estimated 6.2 million African internet addresses worth $150 million from African Network Information Center (AFRINIC) - a non-for-profit responsible for managing the continent's internet registry– allegedly by a former executive of AFRINIC in collusion with other accomplices. This incident has been viewed as an indicative of a broader tendency of African leaders to downplay cyber threats— at considerable cost to economic and national security [3].

[1] https://www.cybrary.it/blog/communicating-cybersecurity-performance-to-corporate-executives/

[2] https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

[3] https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

Africa's Top 8 Cybersecurity Challenges

07 Participation in Global Cybersecurity Activities & Cyber Diplomacy

Poor visibility and engagement in global cybersecurity forums was another challenge pointed out by stakeholders during the workshop at the Hague. Currently, African nations are largely underrepresented and lack prominent voices in international discussions around cybersecurity. For instance, African countries have been largely absent from the evolving UN processes on cyber norms development over the last two decades [1]. Between 2004 and 2021, only 9 out of 54 African nations held membership in the UN GGE on Cybersecurity.

Stakeholders in the Workshop at the Hague agreed that though there have been initiatives by African states towards Cyber Diplomacy- such as the 2014 Malabo Convention on Cyber Security and Personal Data Protection, and the 2019 African Peace and Security Council commitment to develop a Continental Cyber Security Strategy, majority of African countries currently still show little commitment to Cyber Diplomacy.

The establishment of the United nations OEWG on Cybersecurity provides a good opportunity for all countries to express their views. However, only a few states such as Algeria, Egypt, Ghana, Kenya, Morocco, Nigeria, South Africa, Uganda and Zimbabwe have been actively contributing to the OEWG discussions. Again, since the adoption of the Malabo convention by AU member states in 2014, only 9 countries have ratified the convention as of January 2022. Furthermore, only 6 African countries have acceded to the Budapest convention as of January 2022. The limited participation of African players in cyber diplomacy leads to the formation of cyber norms that do not always sufficiently reflect the very needs of resource constrained African states, further making it more difficult for African states to implement the norms [1].

In the face of rising cyber-attacks to critical infrastructures, data breaches, cybercrime, cyber espionage, online theft and pilferage of trade secrets, and offensive cyber operations carried out by state and non-state actors, cyber diplomacy holds the key to mitigate cyber aggression and the escalation of conflicts [2]. The importance of Cyber diplomacy on the wider global level is further showcased by the many cooperation between international key players, for example, the US-China Cyber Agreement 2015 [2].

08 Secure Procurement and Technology Self-Sufficiency

There have been concerns of backdoors deliberately built into technologies exported to Africa. In 2020, there were reports of malicious codes preinstalled on 53,000 Chinese manufactured cell phones sold in Africa [3]. Prior to that in 2017, it had been reported that adware, information-stealing malware and ransomware were found pre-installed along the supply chain on devices belonging to people working in critical infrastructure sectors in some undisclosed countries [4]. Again, these could possibly be African countries. There have been several other reports of malware installation along the supply chain, and this continues to be a global cybersecurity problem which poses threat to various forms of devices including IoT devices [5]. Insecure procurement exposes African countries to multiple risks including cyber espionage and critical infrastructure sabotage, threatening the sovereignty of African nations. It was reported in 2018 that all information on servers in the African Union headquarters was being routinely transmitted to Shanghai, China, enabling the Chinese bad actors to continuously spy on African Union. This is so far reaching partly because of China's role in providing Information Technology infrastructure for AU [6]. Pegasus malware, one of the most sophisticated cyber espionage software was also reported in 2021 to have been discovered on systems in 11 African countries [6].

During the workshop at the Hague, representatives of multiple African countries and stakeholder groups emphasized the importance of ensuring that there are no backdoors on technology frameworks/ products supplied or delivered by third-parties.

The stakeholders further attributed this challenge to over dependency on technology importation and lack of effective disclosure and vetting processes for vendors within contractual agreements. As one delegate aptly put: "We should shy away from being only consumers. We should establish our own products." Other notable cybersecurity gaps paving way for the persistence of this challenge in the continent are inadequacy of government regulations, guidelines and standards for procurement of critical infrastructure, poor monitoring, evaluation and control, and limited expertise and efforts towards coordinating the implementation of laid out frameworks for secure procurement.

[1] https://www.itnewsafrica.com/2020/10/the-state-of-cybersecurity-in-africa/

[2] https://guardian.ng/news/nigeria-announces-twitter-ban-on-twitter/

[3] https://www.bbc.com/news/technology-53903436

[4] https://threatpost.com/38-android-devices-infected-with-malware-preinstalled-in-supply-chain/124275/

[5] https://www.securityweek.com/iot-devices-major-manufacturers-infected-malware-supply-chain-attack

[6] https://africacenter.org/spotlight/africa-evolving-cyber-threats/

High Priority Cybersecurity Challenges of Africa

Top 5 priority Challenges by Region

S/N	CENTRAL AFRICA	EASTERN AFRICA	NORTHERN AFRICA	SOUTHERN AFRICA	WESTERN AFRICA
1	**CYBERSECURITY TRAINING AND AWARENESS** Cybersecurity appears to still be an unfamiliar topic in the region as the level of cyber awareness, opportunity for formal cybersecurity training and cyber cultural practices remain very low	**CYBERSECURITY AWARENESS AND CULTURAL PRACTICES** Despite notable efforts towards cyber capacity development, Eastern Africa is still one of the most successfully attacked regions owing to poor cybersecurity awareness and cultural practices	**CYBERSECURITY CULTURAL PRACTICES** Like its Eastern and Western African counterparts, Northern Africa, though the most cyber mature African region, still ranks among the most successfully attacked mainly due to poor cybersecurity cultural practices	**CYBERSECURITY AWARENESS AND CULTURAL PRACTICES** With South Africa- a leading economy in Southern African being the most attacked African country in 2021, the region continues to be successfully attacked due to poor cybersecurity awareness and cultural practices	**CYBERSECURITY TRAINING AND CULTURAL PRACTICES** Like Eastern Africa, Western Africa, despite cyber capacity development strides, ranks among the most successfully attacked mainly due to limited opportunity for formal cybersecurity education, inadequate awareness and poor cultural practices
2	**CYBERSECURITY STRATEGY** No country in the region is known to have developed a national cybersecurity policy and strategy, which is the very foundation for cyber capacity building	**CYBERSECURITY STRATEGY** Majority of Eastern African countries still lack a cybersecurity policy and strategy which is the starting point for cyber capacity development	**COORDINATION/ IMPLEMENTATION MECHANISM** Though Northern Africa has made notable efforts on cyber capacity development, there is lack of implementation mechanism in many of the countries	**CYBERSECURITY LEGISLATION** Majority of the countries in the region do not have a cybercrime law making it difficult to prosecute cyber criminal activities	**COORDINATION/ IMPLEMENTATION MECHANISM** Implementation mechanism such as coordinating body for strategy implementation and forensics unit for effective cybercrime investigation also lack in Western Africa
3	**CYBERSECURITY LEGISLATION** Many of the countries in the region have no cybercrime law, giving room for cybercrime to flourish and making it challenging for cyber criminal activities to be prosecuted and discouraged	**COORDINATION/ IMPLEMENTATION MECHANISM** Implementation mechanism such as coordinating body for national cybersecurity strategy implementation and forensics unit for effective cybercrime investigation are largely lacking in Eastern African countries	**MULTILATERAL CYBER DIPLOMACY COMMITMENT** A large number of Northern African countries, like other African regions, are yet to engage in notable multi-lateral cyber diplomacy activities such as ratification/ accession to the Budapest and Malabo conventions	**COORDINATION/ IMPLEMENTATION MECHANISM** Implementation mechanism such as coordinating body for strategy implementation, specialized cybercrime prevention unit and forensic investigation unit also lack in many Southern African states	**INTELLIGENCE SHARING FRAMEWORK** A large number of Western African countries still lack a national incident response team and majority of the countries in the region are yet to identify their critical infrastructure operators and set procedures for information exchange between the various stakeholders
4	**INTELLIGENCE SHARING FRAMEWORK** All Central African countries except one lack a national incident response team and no country in the region is represented in FIRST, making it difficult to benefit from international intelligence sharing. No country in the region is known to have formally identified its critical infrastructure operators or set procedures for sharing intelligence between the various stakeholders	**MULTILATERAL CYBER DIPLOMACY COMMITMENT** Though many Eastern African countries have signed bilateral cybersecurity agreements with others and have hosted or co-organized regional/international cyber drills, no significant commitment is seen within Eastern African countries towards notable multi-lateral cyber diplomacy activities such as ratification/ accession to the Budapest and Malabo conventions	**TECHNOLOGY SELF-SUFFICIENCY AND SECURE PROCUREMENT** Like Other African regions, Northern African countries are dependent on developed nations for procurement of critical infrastructure, yet have also largely failed to develop and implement secure procurement standards even in the face of rising concerns about cyber espionage	**INTELLIGENCE SHARING FRAMEWORK** Many Southern African countries lack a national incident response team and two out of ten countries in the region are represented in FIRST, making it difficult to benefit from international intelligence sharing. Majority of countries in the region are yet to formally identify their critical infrastructure operators or set procedures for sharing intelligence between the various stakeholders	**MULTILATERAL CYBER DIPLOMACY COMMITMENT** Many West African countries, despite having hosted regional/international cyber drills and executed international cyber agreements, like their Eastern African counterparts, are yet to engage in notable multi-lateral cyber diplomacy activities such as ratification/ accession to the Budapest and Malabo conventions
5	**MULTILATERAL CYBER DIPLOMACY COMMITMENT** Many Central African countries are yet to engage in notable multi-lateral cyber diplomacy activities such as ratification/accession to the Budapest and Malabo conventions	**TECHNOLOGY SELF-SUFFICIENCY AND SECURE PROCUREMENT** Eastern African countries are dependent on China and other countries for procurement of critical infrastructure, yet have largely failed to develop and implement secure procurement standards even in the face of rising concerns about cyber espionage	**INTELLIGENCE SHARING FRAMEWORK** While all Northern African countries have national incident response teams who are either members of FIRST or AfricaCERT or both through which cyber intelligence is shared internationally, most of the countries in the region are yet to identify their critical infrastructure operators for effective intelligence sharing between various stakeholders	**MULTILATERAL CYBER DIPLOMACY COMMITMENT** Though some countries have signed international cyber agreements and organized cyber drills, Like other regions, many Southern African countries are yet to engage in notable multi-lateral cyber diplomacy activities such as ratification/ accession to the Budapest and Malabo conventions	**TECHNOLOGY SELF-SUFFICIENCY AND SECURE PROCUREMENT** Like Eastern Africa, Western African countries are dependent on developed nations for procurement of critical infrastructure, yet have also largely failed to develop and implement secure procurement standards even in the face of rising concerns about cyber espionage

Conclusion, General Recommendations, and Proposed GFCE Initiatives

Conclusion and General Recommendations

Conclusion

It is noteworthy that efforts have been made by African countries towards cyber capacity building. The level, however, differs from country to country and from region to region, with the least and highest observed in Central Africa and Northern Africa, respectively. One way to explain this variation is the differences in leadership commitment, cultural practices, knowledge and skills, resource availability, cooperation and intelligence sharing, among others, in relation to cybersecurity. These enabling factors are generally underdeveloped across several African countries, and is mainly responsible for the lack of basic CCB building blocks such as comprehensive national cybersecurity strategy, appropriate cybercrime laws and cybersecurity standards observed in many African states, including leading Africa economies. The cyber security maturity gap in African has therefore created opportunities for threats and threat actors to continue to flourish in the continent with weak resistance/defence capabilities, turning Africa into a threat harbour. Nevertheless, African stakeholders are becoming more aware of this situation as is evident in the continuous efforts towards improvement witnessed in most African states. However, the fast evolving technological changes and attendant cyber threat landscape call for an acceleration in cyber capacity building efforts by African states. To achieve success, African nations must prioritize cybersecurity and focus on addressing the root causes that sabotage sustainable growth in cyber capacity. Most importantly, African states must act now.

General Recommendations

The following are aimed towards addressing the identified 8 cybersecurity challenges in Africa:

01 Commitment to Cybersecurity Culture and Education

- Cybersecurity topics should be introduced in primary education to instill good cyber practices in the next generation
- Cyber curriculum should be created for all levels of education
- Cybersecurity course teachers should be trained
- Nations should share knowledge of cybersecurity programmes
- Governments should create national cyber awareness programmes
- There should be more cyber awareness programmes/campaigns by governments, private-sectors and civil societies
- Organizations should develop/adopt information security policies and regularly conduct internal cybersecurity awareness and audits
- Organizations should train dedicated information security teams
- There should be national cybersecurity training progammes for CNI operators in different sectors and for the public sector
- There should be cybersecurity training targeted at SMEs, children and other vulnerable groups

02 Development and Implementation of Robust Cybersecurity Strategy

- Nations should develop comprehensive cybersecurity strategies following a risk-based approach that takes the national cybersecurity threats into consideration
- There should be action plans with clear timelines and resource allocation for implementing national cybersecurity strategy
- Cybersecurity strategy should be regularly updated to meet rapidly changing technological landscape

03 Strategic Coordination and Implementation of National Cybersecurity Programmes

- There should be a government body specifically responsible for coordinating implementation of national cybersecurity strategy
- Frameworks should be developed for audit and effective monitoring/ evaluation of cybersecurity strategy implementation
- There should be government bodies for developing/overseeing compliance with cybersecurity frameworks and issuing sanctions
- Clear responsibilities should be assigned for implementing strategies E.g. creation of cybercrime prevention unit, national DPO, etc
- Clear responsibilities should be assigned for monitoring strategy implementation
- There should be adequate budget/ resource allocation for cybersecurity strategy implementation

04 Development of Robust Legal Framework for Cybersecurity

- National legislators should enact adequate cyber laws such as cybercrime law and data protection law
- Existing cyber laws should be reviewed for adequacy by lawmakers in consultation with cybersecurity stakeholders and amended as required
- Cyber law enforcement officers, judges and other relevant stakeholders should be adequately trained and equipped to effectively combat, investigate and prosecute cybercrime
- There should be inter-state agreements for joint efforts in legally combating cybercrime

Conclusion and General Recommendations

General Recommendations

05 Implementation of Intelligence Sharing Framework

- Secure channel should be established for information sharing with clearly defined protocols for different sectors such as banking, telecoms, aviation, etc
- A responsibility for information sharing and incident reporting that is well-known to various stakeholders and citizens should be established
- National and sectoral incident response teams with regional and international cooperation should be created
- Information should be shared among stakeholders on a need-to-know basis
- Framework for information sharing offering appropriate legal protection for all stakeholders should be established both at national and sectoral levels
- There should be adequate tools, training programmes and regular cyber drills for incident response teams
- There should be clear plans and procedures for incident response and disaster recovery both at national and sectoral levels

06 Prioritization of Cybersecurity in Leadership

- Technical experts should adequately communicate the necessity of cybersecurity to leaders to build political will
- The executive leadership of companies and critical government agencies should include a Chief Information Security Officer responsible for developing, effectively communicating and implementing the company/ agency's cybersecurity vision and strategy
- Cybersecurity should be part of the defence strategy and national emergency response strategy
- Cybersecurity frameworks should be adopted/developed for critical infrastructure sector operators with adequate sanctions on non-compliant operators
- Cyber awareness should form part of national media /information communication campaigns/programmes
- Cybersecurity should form part of the national budget

07 Prioritization of Commitment to Global Cyber Activities and Cyber Diplomacy

- An African alliance on cybersecurity should be created so goals and processes would be harmonized to aid nations further behind to develop capacities faster and enable African nations present themselves as a unified bloc and have stronger power in international negotiation forums
- Nations should showcase their success stories at the international scene to improve visibility
- Cyber diplomats with requisite skills and trainings should be appointed to constitute specific branches of foreign offices
- There should be capacity building programmes for cyber diplomats on international cyber norms and diplomatic approaches
- Cyber diplomats should work to encourage government officials to ratify treaties and agreements
- There should be more coalition between African countries

08 Implementation of Secure Procurement Framework and Encouragement of Local Technology Development

- Standards should be developed and implemented for vetting vendors through audits or external certifications of good practice when outsourcing contracts
- Audits and security tests should be conducted on technology infrastructure during the procurement process
- Local production capacity should be built from ground up and there should be support for local startup companies

Proposed GFCE Initiatives

Proposed GFCE initiatives

Based on our recommendations, we have drawn the following list of initiatives that can be pursued by the GFCE to bridge the gap in cyber capacity and further advance cyber resilience in the African region. These initiatives should be respectively targeted at the countries with gaps in the associated capacity areas, especially in the regions specified as high priority:

Cybersecurity Culture, Awareness and Education Development Initiatives

ED-1 Develop cybersecurity curriculum for secondary & tertiary institutions

High Priority Regions	1. Central Africa 2. Eastern Africa 3. Western Africa
Deliverables	1. School curriculum 2. Implementation plan

The GFCE should consider partnering with relevant government agencies in beneficiary countries to develop cybersecurity curriculum for schools, and a clear plan with timeline for operationalizing the curriculum. For secondary schools, the curriculum may be developed as standalone or as part of an already existing curriculum for teaching the fundamentals of technology. For tertiary institutions, the curriculum can be developed as part of the non-programme specific courses offered under general-studies.

ED-2 Conduct train-the-trainer workshop for cybersecurity teachers in public schools

High Priority Regions	1. Northern Africa 2. Southern Africa
Deliverables	1. Workshop sessions 2. Free training materials

The Forum should consider conducting train-the-trainer workshop sessions for cybersecurity teachers in public secondary and tertiary schools. Also, the teachers should be supported with free training materials for continuous capacity building. This initiative should be targeted at countries with existing arrangements for teaching cybersecurity in public institutions. Additionally, this initiative can be implemented alongside ED-1, thus preparing and equipping teachers towards the introduction of cybersecurity curriculum to institutions.

ED-3 Establish National Cyber Awareness programme targeted at vulnerable groups

High Priority Regions	1. Central Africa 2. Eastern Africa 3. Western Africa
Deliverables	1. Delivery channels 2. Awareness content 3. Training workshop

The GFCE should consider partnering with relevant government organisations to establish cyber awareness programmes and campaigns targeted at women, children, elderly, SMEs and other vulnerable groups. Tailored content such as informational videos, materials and insights should be developed. Delivery channels such as website, radio, television, phone caller tunes, bill boards, signages, etc should be establish/aligned based on access and availability. Training sessions should also be conducted to equip local delivery team.

Cybersecurity Policy and Strategy Development/ Implementation Initiatives

PS-1 Draft/ review national cybersecurity policy and strategy

High Priority Regions	1. Central Africa 2. Eastern Africa
Deliverables	1. Cybersecurity policy 2. Cybersecurity strategy

The GFCE should consider helping AU member states to develop national cybersecurity policy and strategy to define the roadmap for cyber capacity building in states at the early stage of CCB. This can be achieved by partnering with a relevant government body which may be ad-hoc where a state is yet to fully establish clear responsibilities for cybersecurity coordination. Furthermore, the forum should consider helping to review cybersecurity policy and strategy for member states where this already exists but may not be adequate.

PS-2 Develop national cybersecurity strategy implementation plan

High Priority Regions	1. Central Africa 2. Southern Africa
Deliverables	1. Implementation plan

Strategy implementation plan should also be developed for member states who already have a cybersecurity strategy. Also this initiative can be implemented alongside PS-1 for member state where cybersecurity policy and strategy is yet to be established. The implementation plan should outline clear roles, accountability and responsibilities, timelines, resource requirements, performance indicators, among others for effectively implementing the cybersecurity policy and strategy.

PS-3 Assist in the establishment of cybersecurity coordinating bodies

High Priority Regions	1. All African Regions
Deliverables	1. Target operating model 2. Implementation plan 3. Workshop sessions

The Forum should consider assisting African states to develop a target operating model for cybersecurity coordinating body. The model should detail the functional processes, roles and skillsets, governance frameworks, and technology requirements for the smooth operation of the coordinating body as an organization. Additionally, a clear plan for the establishment of the body should be developed. Workshop sessions should be conducted to gain inputs from stakeholders as well as to gain alignment and deliver the final model.

Proposed GFCE Initiatives

Proposed GFCE initiatives

Legislation and Legal Framework Development Initiatives

LS-1 Review and recommend changes to existing cybercrime and data protection laws

High Priority Regions	1. All regions
Deliverables	1. Recommendations report

The GFCE should consider helping AU member states who already have existing but inadequate cybercrime/data protection law to propose reviews to the exiting law. This can be delivered in a recommendations report highlighting recommended changes to the law with justifications for the recommendations. The forum can partner with the nation's cybersecurity coordinating body, data protection authority and/or other relevant stakeholders to deliver this initiative.

LS-2 Draft and propose new cyber crime and data protection laws

High Priority Regions	1. Central Africa 2. Eastern Africa 3. Southern Africa
Deliverables	1. Draft legislation 2. Recommendations report

For states where cybercrime and/or data protection law is missing, the GFCE can partner with relevant government organizations to deliver draft cybercrime/ data protection laws. The government body, working with cybersecurity, judiciary, legislative and other key stakeholders, will be responsible for taking the proposed law through further stages of enactment. Additionally, a recommendations report should be delivered to provide justifications for the proposed law, build political will, and promote acceptance and enactment.

LS-3 Carry out campaigns targeted at the public to familiarize and create awareness on cyber laws

High Priority Regions	1. Northern Africa 2. Western Africa
Deliverables	1. Awareness campaign

For states where adequate cybercrime and/or data protection laws exist, the GFCE can undertake a campaign to create awareness to the general public on the laws. The campaign should be delivered over a defined timeline through appropriate channels, considering availability and access to the channel to deliver maximum impact. The campaign should be delivered in partnership with relevant government bodies such as the judiciary council and ministry of information.

LS-4 Conduct capacity building workshops for the judiciary

High Priority Regions	1. Northern Africa 2. Western Africa
Deliverables	1. Workshop session 2. Free reference materials

For African states where cybersecurity laws exist, the GFCE can organize workshop sessions to engage with judicial actors to improve and strengthen their capacities in handling cybercrime and data breach cases.

LS-5 Conduct training workshop for law enforcement agencies

High Priority Regions	1. Northern Africa 2. Western Africa
Deliverables	1. Workshop session

For states with adequate cybercrime laws, the GFCE can carryout specialized training workshops for the law enforcement agencies to cover information sharing, legal awareness, early response, among other topics to improve and strengthen their capacities in investigating cybercrime and enforcing cybercrime laws.

LS-6 Help establish forensics investigation laboratories

High Priority Regions	1. All regions
Deliverables	1. Lab facility/ equipment 2. Training workshop

The Forum should consider supporting AU member states with facilities and/or equipment for carrying out digital forensic investigation. This should be delivered to an appropriate law enforcement agency such as the police. Additionally, specialized training workshops on digital evidence handling, equipment operation and other related topics should be conducted for the local team who will be responsible for operating the laboratory.

Proposed GFCE Initiatives

Proposed GFCE initiatives

Critical National Information Infrastructure (CNII) Protection and Intelligence Sharing Initiatives

CI-1 Help identify and recommend CNII for designation

High Priority Regions	1. Central Africa 2. Western Africa
Deliverables	1. Proposed CNII list

The GFCE should consider helping AU member states to identify critical national information infrastructure (CNII). CNII should be identified in partnership with relevant government and private sector stakeholders after which report is delivered to the appropriate government authority listing and recommending CNII for designation. CNII should be categorized based on the CNII sector to enable implementation of sectoral CNII protection measures.

CI-2 Conduct National Cyber Risk Assessment

High Priority Regions	1. Southern Africa 2. Northern Africa 3. Eastern Africa
Deliverables	1. CNII risk report

For nations where CNII has been designated by the government, the GFCE can help CNII regulators and operators to identify CNII risk by facilitating a multi-stakeholder national cyber risk assessment exercise. Based on outputs from the assessment, CNII risk report should be delivered to the CNII protection authority or appropriate government body to inform decisions on the implementation of risk mitigation and CNII protection measures.

CI-3 Develop Critical National Information Infrastructure Protection Plan (CNIIP)

High Priority Regions	1. All regions
Deliverables	1. CNIIP

The GFCE can help AU member states to develop a critical national information infrastructure protection plan (CNIIP) to outline the requirements and responsibilities for CNII protection. This initiative can be delivered alone where CNII is already designated or identified, or alongside CI-1 where CNII is yet to be identified.

CI-4 Establish audit and monitoring framework for CNII protection

High Priority Regions	1. All regions
Deliverables	1. CNII audit/ monitoring framework

The GFCE can help AU member states to develop a framework for monitoring and auditing critical national information infrastructure operations at national and sectoral levels. The framework may include CNII auditing and monitoring procedures, minimum cybersecurity standards to be obtained by CNII operators, required job roles and minimum requirements of CNII regulators etc. This initiative can be delivered alone where CNII is already designated or identified, or alongside the CI-1 initiative where CNII is yet to be identified.

CI-5 Conduct training sessions for CNII regulators and operators on CNII protection

High Priority Regions	1. Southern Africa 2. Northern Africa 3. Eastern Africa
Deliverables	1. Training workshop

For nations where CNII has been designated by the government, the GFCE should consider organizing training workshop targeted at CNII regulators and operators to build their capacity on CNII protection. The sessions should focus on CNII regulation best practices, administrative and technical controls for securing CNII, standards and best practices for secure procurement of CNII, among other key topics.

CI-6 Establish annual national CNII protection summit

High Priority Regions	1. Southern Africa 2. Northern Africa 3. Eastern Africa
Deliverables	1. Operating model 2. One year action plan

For nations where CNII has been designated, the GFCE should consider establishing an annual summit for stakeholders including regulators and operators to share knowledge on CNII protection topics. An operating model should be developed for the proposed summit and delivered to the relevant government body detailing the goal, objectives, stakeholders and key activities to be involved in the summit. An action plan should also be developed and delivered to host the summit for the first one year.

Proposed GFCE Initiatives

Proposed GFCE initiatives

Critical National Information Infrastructure (CNII) Protection and Intelligence Sharing Initiatives

CI-7 Help establish national/ sector CSIRT/CERT

High Priority Regions	1. Central Africa 2. Western Africa
Deliverables	1. Target operating model 2. Operating frameworks

The GFCE can help African states establish national or sectoral CSIRTs/ CERTs by delivering a target operating model to outline the processes, roles/ skillsets, technologies and governance framework for the operation of the CSIRT/ CERT. Sectoral CSIRTs/CERTs should target key CNII sectors. Also, operating frameworks such as incident categorization/ management framework and intelligence sharing framework should be delivered to cover guidelines and hierarchy for wider communications regarding national incidents.

CI-8 Conduct capacity building workshop for CERT/ CSIRT

High Priority Regions	1. Eastern 2. Northern Africa 3. Southern Africa
Deliverables	1. Workshop sessions

For nations where CSIRT/CERT is already in operation, the GFCE can deliver capacity building workshops to both national and sectoral CSIRTs/CERTs to help build capacity of the stakeholders in incident response, threat intelligence, intelligence sharing and other key topics. This initiative can be conducted as part of CI-7 for nations where national/ sectoral CSIRT/CERT is yet to be established.

CI-9 Help CERTs/CSIRTs to join International Intelligence Sharing bodies like FIRST

High Priority Regions	1. Central Africa 2. Western Africa
Deliverables	1. Successful admission to intelligence sharing bodies

For nations where CSIRT/CERT is already in operation but yet to join intelligence sharing bodies such as FIRST, AfricaCERT, OIC-CERT, GFCE, etc, the GFCE should consider leveraging its network to sponsor membership and help CSIRTs/CERTs meet other requirements of intelligence sharing bodies. This initiative can also be conducted as part of CI-7 for nations where national/ sectoral CSIRT/CERT is yet to be established.

Cyber Diplomacy Development Initiatives

DP-1 Develop capacity building framework for country cyber representatives

High Priority Regions	1. Central Africa 2. Southern Africa
Deliverables	1. Capacity building framework 2. Workshop session

The GFCE can help develop capacity building framework for stakeholders who represent countries at different cybersecurity bodies. Additionally, capacity building workshop sessions should be facilitated to engage with the stakeholders to strengthen and improve their knowledge and skills of diplomatic approaches.

DP-2 Conduct capacity building workshop for key stakeholders involved in ratifying cyber norms

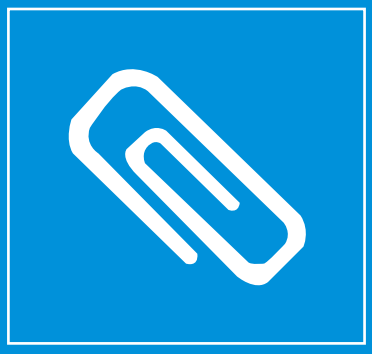
High Priority Regions	1. All regions
Deliverables	1. Workshop sessions

The GFCE should consider facilitating capacity building work for key government stakeholders involved in ratifying/ acceding to international cyber norms in order to sensitize the stakeholders, encourage them, and build political will for ratifying or acceding to cyber norms such as the Budapest Convention and the Malabo convention.

DP-3 Support AU member states to host/ participate in regional/ international cyber drills

High Priority Regions	1. All regions
Deliverables	1. Cyber drill/ exercise

The GFCE should consider partnering with relevant government organizations in AU member states to help the member state host or participate in regional or international cyber drills. The GFCE can leverage its network and diplomatic relations to ensure maximum cooperation from other nations/ regions.



Appendix

Appendix

Glossary

ABBREVIATION	MEANING
AfricaCERT	The African Forum of Computer Incident Response Teams
AFRINIC	African Network Information Center
ARCC	Arab Regional Cybersecurity Center
AU	African Union
BEC	Business Email Compromise
CCB	Cyber Capacity Building
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIRT	Computer Incident Response Team
CNI	Critical National Infrastructure
CNII	Critical National Information Infrastructure
CNIP	Critical National Infrastructure Protection
CRC	Cybersecurity Response Committee
CSDA	Cybersecurity Digital Alliance
CSIRT	Computer Security Incident Response Team
CWG-COP	Council Working Group for Child Online Protection
DDoS	Distributed Denial of Service
Dollars	United States Dollars
DPC	Data Protection Centre
DPO	Data Protection Officer
DRC	Democratic Republic of Congo
EG-CERT	The Egyptian Computer Emergency Readiness Team
ESCC	The Egyptian Supreme Cybersecurity Council
FIRST	Forum of Incident Response and Security Teams
GCI	Global Cybersecurity Index
GDP	Gross Domestic Products
GFCE	Global Forum on Cyber Expertise
GGE	Group of Governmental Experts
I-CSSI	The African Institute for Cybersecurity and Infrastructure Security
ICT	Information Communication Technology
INTERPOL	The International Criminal Police Organization
ISOC DRC	Internet Society, Democratic Republic of Congo Chapter
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunications Union
KE-CIRT	The National Kenya Computer Incident Response Team
KPMG	KPMG Professional Services
NC3	National Cyber Command Centre
NC4	The Computer and Cybercrime Coordination Committee
NCC	Nigerian Communications Commission
NCPF	National Cybersecurity Policy Framework
NCSAM	National Cybersecurity Awareness Month
NCSI	National Cybersecurity Index
ngCERT	Nigeria Computer Emergency Response Team
NITDA	National Information Technology Development Agency
OEWG	Open Ended Working Group
OIC-CERT	Organization of the Islamic Cooperation Computer Emergency Response Team
ONSA	The Office of the National Security Adviser
PCI-DSS	Payment Card Industry Data Security Standard
PKI	Public key Infrastructure
POPI Act	The Protection of Personal Information Act
R&D	Research and Development
SME	Small and Medium Enterprises
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development

Appendix

Assessment of Africa's Cyber Maturity Based on Regions- Cybersecurity Domain to Dataset Mapping

DOMAIN	DATASET	
	GCI	NCSI
Cybersecurity Policy and Strategy/ Cyber Diplomacy	A. Organisational Measures	1. Cyber security policy development
CERTS/CSIRT & CIIP/CNIP	B. Technical Measures	CERTS/CSIRT 9. Cyber incidents response 12. Military cyber operations CIIP/CNIP 10. Cyber crisis management 6. Protection of essential services
Legislastion & Legal framework	C. Legal Measures	11. Fight against cybercrime 7. E-identification and trust services 8. Protection of personal data
Awareness, skills and workforce development	D. Capacity Development Measures	2. Cyber threat analysis and information 3. Education and professional development 4. Contribution to global cyber security
Open Internet and cybersecurity standards	B. Technical Measures:	

Appendix

Interviewed Nations/Organisations and Agenda – April/May 2022

In order to gain new insight on current cyber capacity needs and validate our existing knowledge base, KPMG had meetings with representatives of the following countries/organisations:

REGION	COUNTRY/BODY	ORGANISATION/UNIT
West Africa	Ghana	Cyber Security Authority
East Africa	Kenya	Ministry of ICT, Innovation and Youth Affairs
Central Africa	Republic of Congo	Ministry of Posts and Telecommunications
North Africa	Morocco	Moroccan Computer Emergency Response Team
Southern Africa	N/A	N/A
Africa	• Smart Africa • African Union	• Cybersecurity Working Group • Cyber Security Expert Group (AUCSEG)

The agenda of the meeting was as follows:

- **National Cybersecurity approach**: Existing strategies addressing cybersecurity , The specific risk management approaches adopted at national level, The cybersecurity Governance framework within the country, The specific cybersecurity Programs and Initiatives undertaken within each country.
- **Existing and emerging standards**: International, national and (where applicable) state standards adopted cyber standards adopted within region/country
- **Regulation**: Cybersecurity related legislation that exists within the region/country.
- **Enforcement:** Enforcement methods used to enforce the practice of cybersecurity, cybersecurity periodic audit requirements that exist at national level
- **Capacity Building:** Existing cybersecurity capacity building initiatives
- **Cybersecurity Operations:** Cybersecurity Incident reporting requirements and response mechanisms that exist at sector / national level, Presence of agencies or mechanisms at the national level, that assist organizations in identifying cyber threats
- **Cybersecurity Challenges/Bottlenecks :** Current challenges faced while advancing cybersecurity capacity within the region/country
- **Cyber Maturity of the Country**: Discussions on the perceived current cyber maturity level of the country.
- **Advancement initiatives**: Discussions around the region/country's current and planned cyber enhancing initiatives.
- **Way Forward:** Discussions on next steps to be taken to advance cyber within the region/country.

Appendix

Workshop Attendance - November 2021

The following stakeholders attended the 2-day workshop held by the GFCE and Africa Cyber Capacity Building Coordination Committee on CCB in Africa at The Hague Netherlands:

S/N	COUNTRY/ ORGANIZATION	NAME
1	ACBF	Fasil Yilma
2	ACSIS	Aicha Jeridi
3	AfricaCERT	Jean-Robert Hountomey
4	AFRINIC	Arthur Cardinal
5	AFRIPOL	Omar Daas
6	ARTAC	Serge Emile Mbasse
7	AUCSEG	NnennaIfeanyi-Ajufo
		Abdul-Hakeem Ajijola
8	Benin	Miguel Sossouhounto
		Sevi Rodolphe Adjaigbe
9	Botswana	Lesedi Mashumba
		Sinka Matengu
10	Burkina Faso	Palingwende Clovis Arnaud Djigma
		Joag Chrislain Missamou
11	Cameroon	NGA Bertrand Kisito
		NGBWA Arsene Chanel
12	CRASA	Ms. Bridget Linzie
13	Dem Rep of Congo	Mr Eric Armel Ndoumba
		Mr Serge Abel Ongani
14	Eswatini	Mr Wandile Comfort Mhlanga
		Ms. Nokuthula Hlophe
15	Ethiopia	Mr. KassayeTafesse
		Mr. Hannibal Lemma
16	Ghana	Mr Owusu Bediako-Poku
		Mr Samuel AntwiGyekyi
17	Malawi	Mr Paul Katema
		Mr Christopher Banda
18	Mauritania	Didi el Housseine
19	Morocco	Mr. Zakaria Yartaoui
		Mr. Salim Khanfri
20	Mozambique	Lourino Alberto Chemana
		Sergio Henrique Guivala
21	Namibia	Ms. Elizabeth Ujarura Kamutuezu
		Ms. Geneva Hanstein
22	Registry Africa	Lucky Masilela
23	Senegal	Mrs Racky Seye
		Mr. El Hadji Ndiawar Cisse
24	Sierra Leone	Mr. Musa Jalloh
		Hon. Solomon Jamiru
25	Somalia	Mr Abdullahi Guled
26	The Gambia	Mr. Sanusi Drammeh
		Mr. Amadou Bah
27	WATRA	Emanuel Livramento
28	Zambia	Nalucha Imasiku
		Chita Chibesakunda

Appendix

Survey Respondents - August 2021

All AU-member states were invited to respond to a survey on their Cyber Capacity Building Priority (CCB) needs, the following 17 responded:

S/N	COUNTRY
1	Benin
2	Botswana
3	Burkina Faso
4	Republic of Congo
5	Eswatini
6	Ethiopia
7	The Gambia
8	Malawi
9	Mauritania
10	Morroco
11	Mozambique
12	Namibia
13	Rwanda
14	Senegal
15	Sierra Leone
16	Somalia
17	Togo

John Anyanwu
Partner, Cyber and Privacy
KPMG Nigeria
T: 234 803 975 4061
john.anyanwu@ng.kpmg.com

Samuel Asiyanbola
Associate Director, Cyber & Privacy
Mobile : 234 802 501 3893
samuel.asiyanbola@ng.kpmg.com

kpmg.com/socialmedia