1. INTRODUCTION

Africa has begun exploring an agenda on digital transformation in relation to peace and security. Following endorsement by the 2019 Sharm El Sheikh Declaration, in February 2020, the African Union Commission (AUC) adopted the Digital Transformation Strategy for Africa. The African Digital Transformation Strategy has highlighted the need for a greater capacity to detect and mitigate cyber-attacks. According to The Strategy, African Governments responsibility to create an enabling environment with policies and regulations that promote digital transformation across foundation pillars which includes cyber security, is a cross cutting theme of the strategy. Digital transformation offers Africa tremendous opportunities, however, effective, and efficient digital transformation in Africa can only happen in a trusted and secure cyber space.

2. AFRICAN UNION INITIATIVES

Since the adoption of the African Union Convention for Cybersecurity and Personal Data Protection (Malabo Convention) 2014, the AUC has been organising Cybersecurity capacity building workshops, in collaboration with key partners, Regional Economic Communities (RECs) and Member States, to promote Cybersecurity culture provide guidance on cybersecurity policy as well as strengthening Cybersecurity Capacities of Member States. In 2017, the AUC, in cooperation with Internet Society, developed Guidelines on ‘Security of Internet infrastructure in Africa’. Furthermore, the Executive Council of the African Union endorsed in 2018 ‘The AU Declaration on Internet Governance and development of Africa’s Digital Economy’ and adopted cybersecurity as a Flagship project of the African Union Agenda 2063. In furtherance of the cyber governance agenda, in December 2019, the AUC appointed the African Union Cybersecurity Experts’ Group (AUCSEG), composed of 10 members representing all the African regions, whose objective is to provide guidance and recommendations on Cyber policies and strategies to AUC with the aim to adopt, monitor, prevent, mitigate and address current and emerging cyber threats and data misuse.

1 African Union Specialized Technical Committee on Communication and Information Technologies (STC-CICT) Third Ordinary Session, 22 - 26 October 2019, Sharm El Sheikh, Egypt 37590-2019_sharm_el_sheikh_declaration - stc-cict-3_oct_2019_ver2410-10pm-1rev-2.pdf (au.int)
6 African Union Declaration on Internet Governance and Development of Africa’s Digital Economy Assembly/AU/Decl.3(XXX)
7 See Agenda 2063: The Africa We Want. Agenda 2063: The Africa We Want. | African Union (au.int) “Agenda 2063 is the strategic framework for delivering on Africa’s goal for inclusive and sustainable development and is a concrete manifestation of the pan-African drive for unity, self-determination, freedom, progress and collective prosperity pursued under Pan-Africanism and African Renaissance.” As an affirmation of their commitment to support Africa’s new path for attaining inclusive and sustainable economic growth and development African heads of state and government signed the 50th Anniversary Solemn Declaration during the Golden Jubilee celebrations of the formation of the OAU /AU in May 2013. The Agenda 2063 is the concrete manifestation of how the continent intends to achieve this vision within a 50-year period from 2013 to 2063.
deliverables of the AUCSEG include undertaking cybersecurity capacity building initiatives; advising the AUC and African Union member states on Cybersecurity matters,\(^8\) and developing and implementing confidence building measures in line with existing UN Norms. The AUSCEG as part of its mandate established three (3) key working groups – the Cybersecurity Strategy Working Group, tasked with developing a Cybersecurity Strategy for the Continent; the Malabo Convention Working Group- Tasked with reviewing and promoting the ratification of the African Union Cybersecurity and Personal Data Protection, 2014 and; the Child Online Safety Working Group tasked with developing a Child Online Safety Policy for the Continent. Another important step taken by the AUC in close collaboration with the European Union is the launching of the ‘Policy and Regulation Initiative for Digital Africa (PRIDA)’.\(^9\) Building capacity of Africans stakeholder groups in all 55 AU Member States on Internet Governance and Cybersecurity/ Cyber-resilience matters is one of the critical mandates of PRIDA. The AUC has also been efficiently engaged in cooperation strategies with key international regional partners and the sub-regional bodies in Africa such as Economic Community of West African States (ECOWAS) and South African Development Community (SADC). These Sub-Regional bodies have also been effectively involved in cybersecurity capacity building efforts on diverse levels to advance cybersecurity in the region.

At the recently concluded African Internet Governance Forum held in Lilongwe, Malawi from 19th to 21st July 2022, which the African Union Commission is a key stakeholder, an African School of Internet Governance (AfriSIG22) was constituted as a pre-event of the forum for Multistakeholder Consultation on African Participation in the OEWG by Africans. A document which identifies and prioritises African cyber capacity needs was drafted by a group of around 30 individuals from state and non-state institutions involved in cybersecurity from more than 15 African countries.

3. IDENTIFYING AND PROMOTING CYBERSECURITY CAPACITY-BUILDING NEEDS IN AFRICA

As Africa is embarking on flagship initiatives such as Digital Transformation Strategy (DTS) 2020-2030 and the African Continental Free Trade Area (AfCFTA), cybersecurity capacity building is needed to increase adoption, access and facilitate implementation. Cooperation and coordination in addressing Africa’s cyber-related threats is critical. It has become important to involve all relevant stakeholders in building capacity for promoting cybersecurity in the region. Priority areas where cyber capacity building is needed include governance, policymaking, technical tools and infrastructure, digital access and research.

1. The reality of cybersecurity often collides with realities of developing states, particularly for states in the African region which are at the end of the digital divide and lack the capacity, skills and infrastructure to effectively ensure cybersecurity at international standards. It is therefore recommended, that it is necessary to establish and enhance capacity at national levels in Africa. Country specific, strategic and

\(^8\) African Union Cyber Security Experts Group. Terms of Reference 34922-annc-au_cyber_security_expertgroup_tors.pdf; See also African Union Cybersecurity Expert Group holds its first inaugural meeting | African Union.

\(^9\) The “Policy and Regulation Initiative for Digital Africa” (PRIDA) is a joint initiative of the African Union (AU), the European Union (EU) and the International Telecommunication Union (ITU). It is supported by the EU-funded Pan African Programme. See Policy and Regulation Initiative for Digital Africa (PRIDA) (itu.int)
sustainable capacity building is required given the varied cybersecurity maturity levels, local context, political realities and cultural diversity.

2. African institutions require capacity for developing and sharing research methodologies for cybersecurity needs and readiness assessments at national, sub-regional and regional level. This will include conducting comprehensive national cyber-needs assessments to determine gaps and needs of the different actors and stakeholder groups participating in cybersecurity processes.

3. Capacity development for the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII) is needed. It is important to assist African states to establish cybersecurity incidents response teams (CSIRTs) or Computer emergency response teams (CERTs) where they are not yet in place. It is important to also develop and implement mechanisms for national, sub-regional, regional and continental collaboration CSIRTs and CERTs. This includes enhanced capacity for effective communication among response teams, and between them and other stakeholders.

4. African actors also need greater capacity to be able to contribute effectively to UN Processes such as the Open-Ended Working Group (OEWG) and other global cybersecurity initiatives. Awareness raising, inclusion and ensuring transparent approaches towards enhancing participation of African actors and policy makers should be prioritised.

5. Developing comprehensive and efficient cybersecurity strategies, policies, regulations must be prioritised for Africa. It is important to develop capacity for appropriate law-making and cybersecurity legislating in Africa. Specific capacity development is needed to build the awareness and skills required to change the traditional national security centered conception of cybersecurity to a multi-stakeholder people-centered and human rights-based approach towards cybersecurity legislating in Africa.

6. In some instances, the capacity for effective cybersecurity-legislating followed with the capacity for implementing such laws is still a challenge. Such gaps for parliamentarians and policymakers would mean unrealistic cybersecurity strategies. Where African countries have cybersecurity laws, there is still need for capacity to implement them and this includes policymakers, law enforcement officers, prosecutors, and judges.
   i. Law enforcement institutions need capacity building strategies that underscore effective collaboration and mutual legal assistance and the understanding that the prosecution of cybercrime requires the respect of human rights in cybercrime policing strategies.
   ii. Policy makers, Diplomats and Parliamentarians need capacity development to understand the cybersecurity landscape and actors and the involvement of multi-stakeholder groups in shaping appropriate and effective policies which consider best practices and importantly, the UN Norms of Responsible State Behaviour.
   iii. Capacity building is also relevant for the judiciary for understanding and
addressing cybercriminal matters and issues of applicability of digital evidence.

7. An often ignored sector for cybersecurity capacity building in Africa is the civil society groups. Cybersecurity responses in Africa must transcend the traditional notions of security. While governments play the primary role in creating the public policies and laws that regulate and determine cybersecurity measures domestically, it is important to build capacity for African Civil societies so that Africa can leverage multistakeholder partnerships in line with Article 26 of the African Union Convention for Cybersecurity and Personal Data Protection (Malabo Convention) 2014. Civil society is uniquely positioned to advocate for cybersecurity policies based on a human rights approach and can play an important role by monitoring and documenting government and business practices, identifying knowledge gaps, and providing analysis to inform policies and relevant discussions on cybersecurity in the African region.

8. It is important to keep building capacity for understanding the threat landscape in Africa. The achievement of this goal hinges on many challenges. African states’ under-resourced institutions often lack the technical skills, capacities and financial resources to effectively implement cyber policies and enforcement measures. Developing a regional cybersecurity centre like other regions to enhance cross-border cooperation and information sharing will enhance capacity building efforts for cybersecurity in the region. Many African states are yet to design and adopt cybersecurity strategies and hence, need capacity development for drafting and implementing comprehensive national cyber security strategies.

9. Capacity building to advance a culture of cybersecurity leadership in Africa should also be given attention. Capacity building efforts targeted at developing effective and efficient victim response mechanisms is an imperative in the region. It will be beneficial if adequate resourcing for cybersecurity capacity development for citizens through skills development, education and awareness is given adequate attention, including through integrating cybersecurity education into curricula at schools and institutions in Africa.

10. Lastly, Africa must not be excluded in the cybersecurity confidence building initiatives. Capacity building initiatives should further focus on Confidence Building Measures (CBMs) for the African region as has been done in other regions.