Key Issues in Addressing Cybersecurity Challenges on the African Continent[1]

Károly Kassai[2]

Abstract:

This study examines the strategic-level characteristics of the cybersecurity frameworks within African Union Member States. While cybersecurity remains under national jurisdiction, the African Union holds the responsibility to support Member States in developing and maintaining their national capabilities. The paper evaluates the cybersecurity requirements established by the Malabo Convention and presents the supplementary initiatives and programs designed to support its implementation. By detailing the specific elements of national cybersecurity frameworks, the study provides a comprehensive assessment of the current landscape. Finally, the analysis of continental-level organizational structures highlights the key components of strategic and operational support. The overview emphasizes the critical role of the forthcoming African Union Cybersecurity Strategy, as well as the significance of measurement and feedback mechanisms that objectively reflect political-strategic decision-making and practical implementation.

Keywords:
Cybersecurity; Cyber-Governance; Malabo Convention; Security Requirements; National Responsibility.

[1] DOI: 10.12700/jceeas.2026.6.2.469

[2] Section Head, Ludovika University of Public Service, Faculty of Military Science and Officer Training, Department of Military National Security; ORCID: 0009-0009-9398-6158; karoly.kassai@yahoo.com

Introduction

In recent years, cybersecurity and cyberthreats have gained significant prominence in both international news and professional discourse. Illustrative of this trend is the EU Network and Information Security Directive (NIS2 Directive), which established general cybersecurity requirements in 2022, followed by the publication of its implementing regulations in 2024. Subsequent, more specialized instruments include the Cyber Resilience Act (CRA), which sets specifications for manufacturers; the Cyber Solidarity Act, aimed at collective defence and resource-sharing among Member States; and the AI Act, which focuses on the robustness and security of artificial intelligence systems.

While these requirements strengthen the European cybersecurity ecosystem, relatively limited attention has been paid to the African Union's recent ratification (in 2024) of the Convention on Cyber Security and Personal Data Protection (the „Malabo Convention").

Just as the economies, digital infrastructures, and cybersecurity frameworks of European states are heterogeneous, this diversity is equally characteristic of the African continent, albeit with additional, distinct regional features. These specific African characteristics necessitate a strategic-level mapping of the cybersecurity landscape. At this stage, rather than a granular analysis, the objective is to identify the most pertinent cybersecurity elements, enabling readers to discern the area's most relevant to their interests.

The aim of this study is to examine how continental-level framework regulations and support mechanisms provide tools for the development and maintenance of national cybersecurity frameworks. This research is guided by the following hypothesis.

Hypothesis: The cybersecurity frameworks of African countries must be bolstered through balanced, strategic-level procedural and organizational support. This assumption implies that a purely digitalization-driven approach and the exclusive reliance on technical solutions are insufficient for effective resilience.

The study employs qualitative policy research method. This analysis used to explore the regulatory frameworks and measures shaping cybersecurity on the African continent and to identify national-level support organisations. Qualitative policy analysis is supported by a structured comparative inventory, specifically demonstrating the implementation of requirements across the continent.

While economic, financial, and political factors significantly influence a country's cybersecurity posture, this study intentionally abstracts from these variables to focus exclusively on specific cybersecurity issues.

The data collection for this research was concluded on 1 December 2025.

The first chapter identifies the cybersecurity requirements of the African continent and the core elements of the African Union's support programs. The second chapter

provides a brief overview based on selected characteristics, followed by a final chapter offering a high-level synthesis of the relevant supporting organizations.

1. Strategic Context and Cybersecurity Requirements

The Constitutive Act of the African Union serves as the highest-level regulatory instrument, providing the foundational basis for subsequent cybersecurity regulations. The Union's objectives are underpinned by key principles, including sovereign equality, peace and security, the rule of law, human rights, and continental cooperation (African Union, 2000, pp. Art. 3-4.).

This mandate provides the necessary legitimacy to establish continental action frameworks and to advance regulatory harmonization in the field of cybersecurity, thereby supporting the stability and development of Member States.

Building on the high-level objectives of the Constitutive Act, the primary continental regulatory instrument for cybersecurity and data protection is the „Malabo Convention." Adopted in 2014 following several years of negotiation (ALT Advisory, 2022) the Convention entered into force on 8 June 2023, after ratification by the fifteenth Member State, Mauritania (Kaaniru, 2023).

Despite the lengthy adoption process, the Convention represents a critical turning point for African data protection and cybersecurity, signalling a formal commitment from Member States (Ayalew, 2023).

The Convention establishes a comprehensive legal framework aimed at strategically harmonizing three key areas: enhancing trust in electronic transactions, creating a legal foundation for combating cybercrime while strengthening cybersecurity, and establishing a fundamental framework for personal data protection (African Union, 2014). Furthermore, it defines requirements according to key cybersecurity considerations, which Member States are expected to implement based on their voluntary commitments.

Topic	**Requirement**	**Reference** (African Union, 2014)
National Strategy	Development of a national cybersecurity policy and strategy	Article 24
R&D Support	Support for research and development of cybersecurity technologies and solutions	Article 24(1)
Responsible National Authority	Designation of a competent national authority responsible for cybersecurity	Article 25(1) – (2)(f))
National Data Protection Authority (DPA)	Establishment/designation of a National Data Protection Authority	Article 11
National Incident Response Organization (CERT/CIRT)	Establishment/designation of a national Computer Emergency Response Team (CERT/CIRT)	Article 26(1), (3)
Combating Cybercrime	Creation of a legal framework for criminal sanctions against electronic offenses	Articles 28–35

Topic	Requirement	Reference (African Union, 2014)
Cyber Sovereignty	Establishment of a legal framework to exercise jurisdiction over cybercrimes committed within the territory	Article 29(1)
Cyber Resilience	Development of resilience in national systems	Articles 24, 26
Protection of Cyberspace	Introduction of technical and organizational measures to ensure the security of data and systems	Article 25(1), 26(1)
Emergency Procedures	Coordination of national response mechanisms and emergency procedures	Article 26(1), 27
Incident Reporting Obligation	Implementation of measures to facilitate the reporting of cybersecurity incidents	Article 26(1)
Horizontal Obligations	CERT/CIRTs must cooperate with sectoral bodies and the private sector in incident response	Article 26(2) – (3)
Awareness/Training	Promotion of responsible cybersecurity culture and training	Article 27
International Mutual Assistance	Law enforcement authorities must be able to provide international mutual assistance	Article 32
Protection of Fundamental Rights	The cybersecurity framework must not infringe upon the right to privacy	Article 11 – 13, 25(3)

Figure 1: Key Security Requirements of the AU Malabo Convention. Source: Author's own elaboration.

The analysis of these requirements underscores the intent of Member States to move beyond fragmented national approaches.

By embedding cybersecurity and data protection within a framework of continental cooperation and high-level interoperability, the Convention provides a robust legal foundation for the region. Building upon these commitments, further instruments have been developed to support implementation, specifically addressing resource constraints and the varying levels of cyber maturity across African states.

1.1. Strategic Instruments and Supporting Frameworks

The implementation of the Malabo Convention is further facilitated by the *Internet Infrastructure Security Guidelines for Africa (2017)*. Issued jointly by the African Union Commission (AUC) and the Internet Society (ISOC) as a non-binding instrument, these Guidelines aim to mitigate resource constraints and address the varying levels of cyber maturity across the continent. The document identifies four core pillars of security: awareness, responsibility, cooperation, and respect for fundamental rights. Furthermore, the framework promotes the development of national Computer Emergency Response Teams (CERT/CSIRTs), professional capacity-building, and the establishment of regional information-sharing mechanisms, thereby contributing to the enhancement of African cyber resilience (Internet Society, 2017, pp. 13, 15-17).

These Guidelines exemplify how African Member States translate shared principles into coordinated, practical solutions.

Building upon the commitments of the Malabo Convention, the *Digital Transformation Strategy for Africa 2020–2030 (DTS)* serves as a guiding framework for secure and reliable digital development. The Strategy seeks to advance the digital

economy, foster innovation, and strengthen institutional capacities. It incorporates the recommendations of the EU – AU Digital Economy Task Force (European Commission, 2019), with its cybersecurity component intrinsically linked to the objectives of the Malabo Convention. The cybersecurity requirements outlined in the Strategy include:

- *Establishment* of harmonized cybersecurity policies and regulatory frameworks to support risk management and incident response;
- *Operationalization* of national Computer Emergency Response Teams (CERTs) to facilitate rapid reaction and real-time threat detection;
- *Implementation* of cybersecurity awareness and capacity-building programs;
- *Promotion* of public–private partnerships for threat intelligence sharing and the protection of critical infrastructure;
- *Harmonization* of data protection and security measures with international best practices (African Union Commission, 2020, pp. 33-37).

This Strategy demonstrates the Union's holistic approach to digital transformation, where cybersecurity is embedded as a prerequisite for modernization. In alignment with the DTS, an administrative arrangement was signed in December 2024 between the European Commission and the Smart Africa Alliance to explicitly support the African Union's capacity-building initiatives (European Commission, 2024). (The Smart Africa Alliance, created in 2013, is a pan-African initiative that brings together more than 30 Member States to promote digital transformation and wider access to ICT across the continent.)

Following the DTS, the African Union, led by Côte d'Ivoire, developed the *Continental Cybersecurity Blueprint* in 2023. This Blueprint serves as a strategic roadmap for continental cooperation, aiming to advance regulatory harmonization, professional training, and the development of regional CERTs, while ensuring Africa's active role in shaping global cybersecurity norms. This document provided the foundation for the five-year operational strategy of the *African Network of Cybersecurity Authorities (ANCA)*, adopted in 2025, though the strategy itself is not publicly accessible (TechAfrica News, 2025).

The long-term objectives of the DTS are further advanced by the *African Digital Compact (ADC, 2024)*, which defines the fundamental domains for the continent's digital future through specific pillars.

The ADC aims to create an inclusive, resilient, and sustainable digital Africa. Its ten developmental pillars include affordable digital access, infrastructure expansion, digital literacy, and the enhancement of cybersecurity and data protection. Notably, the ADC treats the development and ethical adoption of Artificial Intelligence as a distinct pillar. Furthermore, multi-stakeholder cooperation is emphasized, encapsulated by the African proverb: „*If you want to go fast, go alone; if you want to go far, go together*" (African Union Commission, 2024, pp. 18-36).

Collectively, these pillars solidify the foundations of digital development across African nations; without them, long-term security and global competitiveness remain precarious. Consequently, the African Union has initiated the development of a

Continental Cybersecurity Strategy. In Communiqué No. 1171 (2023), the AU Peace and Security Council outlined measures to accelerate this process, urging Member States to domesticate the Malabo Convention and align it with national legislation (Peace and Security Council, 2023, p. 1).

These strategic efforts are complemented at the operational level by the *ANCA Five-Year Cybersecurity Strategy*, adopted on 4 February 2025. This strategy, though not publicly accessible, establishes a formal framework for collaboration among national cybersecurity authorities to address cross-border threats. Key elements include:

- *Policy and regulatory harmonization* to foster interstate cooperation;
- *Infrastructure strengthening* through the encouragement of national CERTs and information-sharing cultures;
- *Capacity building* via specialized training and education;
- *Public-private partnerships* and multi-stakeholder engagement;
- *Global advocacy* to ensure Africa's influence in international norm-setting (Smart Africa, 2025).

In conclusion, the African Digital Compact and the ANCA strategy illustrate a vital nexus between digital development and operational security. While the ADC establishes the framework for inclusive growth, ANCA provides the operational resilience necessary to counter cross-border threats. This dual approach — integrating development with security — is essential for achieving lasting competitiveness in the global digital landscape.

1.2. Reflections on the Malabo Convention and its Implementation

These reflections not only assess the Malabo Convention itself but also highlight the institutional capacities, political commitments, and technical measures that determine its feasibility and effectiveness across Africa.

A comparative analysis indicates that the Malabo Convention lacks a sufficiently robust framework for mutual assistance and international cooperation, particularly when contrasted with the Council of Europe's Budapest Convention. This limitation risks fragmenting cooperation along sub-regional or bilateral lines and diminishes the Convention's efficacy in addressing cybercrime. To mitigate these deficiencies, the establishment of regional Computer Emergency Response Teams (CERTs) is recommended, supplemented by coordinated measures modelled after European frameworks (Orji, 2018, pp. 91-108).

Furthermore, significant shortcomings are identified in the *ITU Global Cybersecurity Index 2020* report, which underscores persistent challenges such as limited financial resources, a shortage of skilled professionals, and divergences in national regulatory frameworks. These deficiencies contribute to a widening cyber capacity gap between developed and developing nations, undermining the ability of many African states to establish effective CERTs and implement coherent cybersecurity strategies (ITU, 2021, pp. 6-14).

Critical examinations of the Convention's scope also reveal that it does not adequately address emerging threats such as cyberterrorism, hacktivism, cyberespionage, and cyberwarfare. Moreover, historically weak political commitment — evidenced by the fact that only thirteen Member States had ratified the instrument by 2022 — delayed its entry into force for nearly a decade (Akamo, 2022, pp. 6-12).

An analysis of Africa's cybersecurity landscape published in 2022 highlights that the continent's primary challenges are rooted in governance limitations, legal fragmentation, and institutional capacity gaps. A low level of cybersecurity culture and professional education results in persistent vulnerabilities, while many national strategies either remain absent or lack adequate implementation mechanisms. Fragmented legal frameworks and weak enforcement further hinder effective responses to cybercrime, a problem compounded by limited intelligence-sharing channels. Additionally, insufficient leadership commitment and low participation in global cyber-diplomacy reduce the continent's ability to assert its interests in international norm-setting processes. Finally, non-transparent procurement practices and limited technological self-reliance sustain long-term external dependencies (KPMG Advisory Services, 2022, pp. 24-25).

Similarly, comprehensive scholarly research attributes the vulnerability of Africa's cybersecurity environment to institutional and infrastructural deficiencies that increase exposure to modern cyberattacks. Fragmented responsibilities and limited private-sector involvement weaken incident response; moreover, the obsolescence of critical systems increases risk, as new technologies are often introduced without adequate security controls. The lack of legal harmonization and the insufficiency of human resource and education systems further undermine the sustainable cyber resilience (Dér, 2025, pp. 37-39,40-45).

The Malabo Roadmap offers further critical remarks, noting that the Convention has suffered from political inertia. It is characterized as being simultaneously over-inclusive and under-inclusive: while bundling together diverse policy areas, it lacks the granular detail and enforcement mechanisms necessary for practical implementation. Some critics also argue that it reflects excessive European influence, approximating EU data protection regimes without sufficient adaptation to specific African contexts (ALT Advisory, 2022, pp. 9-10).

Structural deficiencies continue to hinder effective implementation. The diversity of legal systems complicates harmonization, while the limited capacity of data protection authorities weakens oversight. Additionally, the persistent digital divide, particularly in rural areas, restricts infrastructure access and obstructs the deployment of cybersecurity measures (Bouke M A, 2023, pp. 7-9).

Regionally focused examination observes that African cyber governance remains constrained by political fragmentation and institutional gaps. The delayed ratification of the Malabo Convention, combined with contradictory national legislation, undermines the establishment of a unified framework. Sovereignty concerns and limited engagement in global governance further prevent states from building the trust necessary for effective implementation (Ifeanyi-Ajufo, 2023, pp. 152-154).

Finally, the extended ratification process (2014 – 2023) has compromised the Convention's credibility as a continental framework. Many AU Member States have already adopted more robust national or regional data protection regimes, reducing the perceived necessity of the Convention. Furthermore, its provisions are increasingly viewed as outdated, failing to address contemporary challenges such as artificial intelligence, cross-border data flows, and cloud computing (African Researchers Magazine, 2025).

1.3. Synthesizing the Strategic Landscape

Following the adoption of the Malabo Convention, the subsequent decades witnessed an acceleration of AU level strategies and development programs. It is evident that the strategic considerations presented, the requirements embedded in the Convention, and the following initiatives collectively lay the foundations for a comprehensive African cybersecurity framework.

By way of analogy, the EU Directive on Security of Network and Information Systems (NIS2) encompasses similar fundamental content requirements; however, the terminology used is not exactly the same. Figure 2, with its two columns, illustratively shows the similarity.

AU – Malabo Convention, Chapter III. (African Union, 2014)	**EU – NIS2 Directive** (European Union, 2022).
National Strategy (Article 24)	National Cybersecurity Strategy (Article 7)
National Regulatory Authorities (Article 25)	Competent Authorities (Article 8)
National Organizations (e. g. CERT/CIRT) (Article 27, 28)	Computer Security Incident Response Teams (CSIRT) (Article 10)
Resilience (Article 24, 26)	Resilience (Article 7 and 5, 28, 55, 85, 91. p.)
Emergency (Governance, Institutional Framework) (Article 26)	Crisis management system (Article 9)
Education and Training (Article 27)	Training (Article 20, 21)
International Mutual Assistance (Article 32)	Mutual Assistance (Article 37)

Figure 2: Key Elements of the Malabo Convention and the NIS2 Directive. Source: Author's own elaboration.

The alignment of African strategic elements with these internationally recognized requirements confirms the validity of the Convention's objectives.

It is argued that the development and functioning of national cybersecurity frameworks are not merely technical matters. Beyond digitalization and security, their practical effectiveness is shaped by political, legal, and economic decisions, cultural contexts, and resource availability. It may be inferred that the prolonged ratification process, following the initial consensus, was hindered by the emergence of competing

national interests. This underscores the importance of AU level management and the necessity of coordinating diverse national considerations within such a complex regulatory environment.

In light of the aforementioned criticisms, it must be emphasized that international instruments like the Malabo Convention should remain framework-oriented. Essential details must be developed by individual nations during implementation, ensuring that regulations are aligned with national strategic requirements and sovereign internal policies. Regarding the absence of AI and other emerging elements, it should be noted that the Convention already supports the development of three major pillars; further broadening its scope at this stage might diminish its overall effectiveness.

Furthermore, the effectiveness of the adoption process remains critical. Regulatory requirements developed in distinct environments can only be successfully integrated if supporting and oversight mechanisms are available and operational. Practical experience suggests that the elements highlighted in critical reviews — such as regional CERTs and coordinated cyber crisis response — constitute essential operational responsibilities. In addition to regional CERTs, incident management can be bolstered by functional CERTs (e.g., in the energy, finance, healthcare, transportation, and defence sectors), where sector-specific technical requirements can be precisely identified.

The following chapter provides an objective overview of national responses to these requirements. This presentation aims to offer a realistic overview of the cybersecurity landscape across various African countries without engaging in comparative or critical analysis at this stage.

2. Characteristics of National Cybersecurity Frameworks

The overview of the cybersecurity posture across African countries is presented with a broad analytical focus, drawing on components grounded in practical implementation experience. The examined elements include national cybersecurity strategies (or equivalent instruments), cybersecurity legislation, designated supervisory authorities, and operational cybersecurity organizations (CERT/CIRT).

Given the inherent interrelation between cybersecurity and data protection, the existence of data protection legislation and a corresponding oversight authority is also treated as a primary indicator.

In addition to the country names, the comparative analysis reports the global cybersecurity ranking according to the *ITU Global Cybersecurity Index 2024* (International Telecommunication Union, 2024), where Tier 1 (T1) denotes the highest level of maturity. The table also indicates the Malabo Convention ratification status — distinguishing between signatories (s) and those that have fully ratified (r) the instrument (African Union, 2014).

Data for Table 2 were compiled from several specialized sources, including the *FIRST Global CSIRT Directory* (Forum of Incident Response and Security Teams, n.d.) the *UNCTAD Data Protection Legislation Database*, the *ITU National Cybersecurity Strategies Repository*, and *World Bank Digital Governance Profiles* (United Nations

Conference on Trade and Development, n.d.). These were supplemented by an extensive review of national official gazettes and government portals. All entries have been verified as of 01 December 2025.

To ensure consistency in the comparative analysis, Table 3 includes only those countries that meet at least four of the six examined criteria. When examining the presence or absence of the strategy, two legislative acts, and three national organizations, specifying the minimum threshold is critically important. For example, in the absence of a strategy, the lack of a dedicated organizational capability does not yet endanger cybersecurity operability, but further deficiencies can already be critical (including the fact that national organizations cannot operate without legislative foundation). This approach may seem overly critical, but a systemic examination of the operational and cybersecurity framework of information systems can justify the legitimacy of the presented limitation.

To respect country-specific legal traditions, French-language regulatory terms and authority names are preserved in their original form.

Country (GCI tier) Malabo Convention signed or ratified	National Cybersecurity Strategy (or equivalent)	Cybersecurity Act (or equivalent)	Cybersecurity Supervisory Authority (or equivalent)	CERT (or equivalent)	Data Protection Legislation (or equivalent)	Data Protection Authority (or equivalent)
Mauritius (T1) r	National Cybersecurity Strategy (2023–2026)	Cybersecurity and Cybercrime Act (2021) (No. 16 of 2021)	Ministry of Information Technology, Communication and Innovation (MITCI)	Computer Emergency Response Team of Mauritius (CERT-MU)	Data Protection Act (2017) (No. 20 of 2017)	Data Protection Office
Ghana (T1) r	National Cybersecurity Policy and Strategy (2024)	Cybersecurity Act 2020 (Act 1038)	Cyber Security Authority (CSA)	Ghana Computer Emergency Response Team (GhCERT)	Data Protection Act 2012 (Act 843)	Data Protection Commission (DPC)
Rwanda (T1) r	National Cybersecurity Strategy (2024–2029)	Partly: Cyber Crimes Law (No. 60/2018) IT Products Security Proclamation (No. 1310/2023)	National Cyber Security Authority (NCSA)	National Computer Security Incident Response Team (Rw-CSIRT)	Protection of Personal Data and Privacy Law (No. 058/2021)	Data Protection and Privacy Office (DPO)
Egypt (T1) s	National Cybersecurity Strategy 2023–2027	Partly: Law No. 175 of 2018 on Combating Information Technology Crimes	Ministry of Communications and Information Technology (MCIT)	Egyptian Computer Emergency Readiness Team (EG-CERT)	Personal Data Protection Law (Law No. 151 of 2020)	Personal Data Protection Center (PDPC)
Morocco (T1) s	National Cybersecurity Strategy 2030	Loi No. 05-20 relative à la	Direction Générale de la Sécurité des	Moroccan Computer Emergency	Law No. 09-08 (2009) on	Commission Nationale de Contrôle de la

Country (GCI tier) Malabo Convention signed or ratified	National Cybersecurity Strategy (or equivalent)	Cybersecurity Act (or equivalent)	Cybersecurity Supervisory Authority (or equivalent)	CERT (or equivalent)	Data Protection Legislation (or equivalent)	Data Protection Authority (or equivalent)
		Cybersécurité (2020)	Systèmes d'Information (DGSSI)	Response Team (maCERT)	Personal Data Protection	Protection des Données à Caractère Personnel (CNDP)
South Africa (T2) s	National Cybersecurity Policy Framework (NCPF, 2015)	Partly: Cybercrimes Act, 2020 (Act No. 19 of 2020) Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)	State Security Agency (SSA)	South Africa National Computer Security Incident Response Team (ZA-CERT)	Protection of Personal Information Act (POPIA, Act 4 of 2013)	Information Regulator (South Africa)
Nigeria (T3) s	National Cybersecurity Policy and Strategy (NCPS, 2021)	Partly: Cybercrimes Act, 2015 (Act No. 24), amended 2024	Office of the National Security Adviser (ONSA)	Nigeria Computer Emergency Response Team (ngCERT)	Data Protection Act, 2023 (No. 4 of 2023)	Data Protection Commission (NDPC)
Senegal (T3) r	Stratégie Nationale de Cybersécurité du Sénégal (SNC2022)	Partly: Law No. 2008-11 of 25 January 2008 on Cybercrime	Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI)	Senegal National Computer Security Incident Response Team	Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data	Commission de Protection des Données Personnelles (CDP)
Zambia (T2) r	National Cybersecurity Policy (2021)	Cyber Security Act 2025 (Act No. 3 of 2025)	Zambia Cyber Security Agency	Zambia Cyber Incident Response Team (ZCIRT)	Data Protection Act, 2021 (Act No. 3 of 2021)	Data Protection Commission (DPC)
Togo (T2) r	National Cybersecurity Strategy 2024–2028	Law No. 2018-026 on Cybersecurity and the Fight Against Cybercrime (2018)	Agence Nationale de la Cybersécurité (ANCy)	National CERT / Computer Emergency Response Team (CERT-TG)	Loi n°2019-014 relative à la protection des données à caractère personnel	Instance de Protection des Données à Caractère Personnel (IPDCP)
Kenya (T1) s	National Cybersecurity Strategy 2022 – 2027	Partly: Computer Misuse and Cybercrimes Act, 2018 (No. 5 of 2018) Critical Information Infrastructure and Cybercrime Management Regulations, 44 of 2024	National Computer and Cybercrimes Coordination Committee (NC4)	Kenya National Computer Incident Response Team – Coordination Centre (KE-CIRT/CC)	Data Protection Act No. 24 of 2019	Office of the Data Protection Commissioner (ODPC)
Uganda (T3) s	Ugandan National Cybersecurity Strategy 2022–2026	Partly: The Computer Misuse (Amendment) Act, 2022	National Information Technology Authority –	Uganda National Computer Emergency Response	Data Protection and Privacy Act, 2019	Personal Data Protection Office (PDPO)

Country (GCI tier) Malabo Convention signed or ratified	National Cybersecurity Strategy (or equivalent)	Cybersecurity Act (or equivalent)	Cybersecurity Supervisory Authority (or equivalent)	CERT (or equivalent)	Data Protection Legislation (or equivalent)	Data Protection Authority (or equivalent)
		Electronic Transactions Act, 2011 (No. 8 of 2011)	Uganda (NITA-U)	Team / Coordination Centre (CERT.UG/CC)	(No. 9 of 2019)	
Tunisia (T3) s	Stratégie nationale en matière de cybersécurité 2020–2025	Décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité	Agence Nationale de la Cybersécurité (ANCS)	Tunisian Computer Emergency Response Team (tunCERT)	Law No. 2004-63 of 27 July 2004 on the Protection of Personal Data	Instance Nationale de Protection des Données Personnelles (INPDP)
Botswana (T3) n	National Cybersecurity Strategy (2016-2022)	Partly: Electronic Communications and Transactions Act (2014) (No. 14 of 2014)	Botswana Communications Regulatory Authority (BOCRA)	Botswana National CSIRT (BW-CSIRT)	Data Protection (2024) (Act 18)	BOCRA - designated function
Ethiopia (T3) s	National Cybersecurity Policy and Strategy (2020)	Partly: IT Products Security Clearance and Control Proclamation No. 1310/2023. Computer Crime Proclamation No. 958/2016.	Information Network Security Administration (INSA)	Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CERT)	Personal Data Protection Proclamation (2024) (No. 1321/2024).	INSA – designated function
Tanzania (T1) s	Government Cyber Security Strategy (2022–2027)	Partly: Cybercrimes Act, 2015 (No. 14 of 2015)	Tanzania Communications Regulatory Authority (TCRA)	Tanzania Computer Emergency Response Team (TZ-CERT)	Personal Data Protection Act, 2022 (No. 11 of 2022)	Data Protection Commission
Algeria (T3) s	National Cybersecurity Strategy: For a Cyber-Resilient Algeria (2023)	Partly: General rules relating to post and electronic communications (Law No. 18-04 of 13 May 2018) Specific rules on the prevention and fight against ICT crimes (Law No. 09-04 of 5 August 2009)	Agence Nationale de la Sécurité des Systèmes d'Information (ASSI)	Algeria National Computer Emergency Response Team (CERT-DZ)	Law No. 18-07 on the Protection of Individuals in the Processing of Personal Data (2018)	Autorité Nationale de Protection des Données Personnelles (ANPDP)
Mozambique (T3) r	National Cybersecurity Policy and its Implementation Strategy (approved by Resolution No. 69/2021	Partly: Penal Code (Law No. 24/2019) és Electronic Transactions Law (No. 3/2017)	Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC)	Mozambique's National Cybersecurity Incident Response Team (nCSIRT.MZ / CSIRT.MZ)	Partly. Constitution of Mozambique (2004) Electronic Transactions Law (No. 3/2017)	INTIC - designated function
Malawi (T3) s	Malawi National Cybersecurity	Electronic Transactions and Cyber Security	Malawi Communications Regulatory	Malawi Computer Emergency	Data Protection Act, 2024	Data Protection Authority

Country (GCI tier) Malabo Convention signed or ratified	National Cybersecurity Strategy (or equivalent)	Cybersecurity Act (or equivalent)	Cybersecurity Supervisory Authority (or equivalent)	CERT (or equivalent)	Data Protection Legislation (or equivalent)	Data Protection Authority (or equivalent)
	Strategy (NCS) 2019 – 2024	Act, 2016 (Act No. 33 of 2016)	Authority (MACRA)	Response Team (mwCERT)	**(No. 3 of 2024)**	(MACRA – designated function)
Cameroon (T3) s	no officially adopted national cybersecurity strategy	Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cybercriminality in Cameroon	Agence Nationale des Technologies de l'Information et de la Communication (ANTIC)	Cameroon Computer Incident Response Team (CIRT/ANTIC)	Law No. 2024/017 of 23 December 2024 relating to personal data protection	Personal Data Protection Authority (DPA) ANTIC – designated function

Figure 3: Country cybersecurity parameters. Data manually collected; sources current as of 01 December 2025.

It must be noted that the presence of these six parameters does not, in itself, guarantee the effective functioning of cybersecurity and data protection within a given country. This high-level overview, focusing on essential indicators, provides a structural baseline rather than an exhaustive in-depth analysis.

An examination of Figure 2 reveals that twenty countries have already established a significant portion of the legal, strategic, regulatory, and operational structures identified as targets by this study. These nations have developed frameworks that are likely to support the long-term maintenance of cybersecurity through the integration of additional specialized tools.

The geographical distribution of these countries — spanning Northern, Western, Eastern, and Southern Africa — indicates that cybersecurity development is occurring across multiple regional hubs rather than being confined to a single area. This diversity enhances Africa's potential for continental integration, as these leading nations are well-positioned to drive regional and international cooperation. Furthermore, compliance is not limited to the continent's largest economies; smaller states demonstrate that strong political will and institutional organization are sufficient to build a comprehensive framework.

The results presented in Figure 2 suggest that the strategic cybersecurity requirements set by the African Union are not unrealistic, as the necessary tasks are demonstrably achievable. Nearly half of the fifty-five AU Member States have established several of the examined cybersecurity elements, suggesting a positive trend for future national-level development. In many instances, the evolution of a cybersecurity ecosystem begins with criminal law and electronic commerce regulations. A common preparatory step for establishing an independent regulator involves assigning specific functions to an existing state organization (designated authority), while the establishment of incident-handling organizations (CERT/CSIRT) remains a cornerstone of early-stage development.

A notable nuance emerges among the best-prepared countries (Tier 1 classification): Egypt, Morocco, Kenya, and Tunisia have signed the Malabo Convention but have not yet ratified it. This underscores a dual dimension in African cybersecurity: advanced

national preparedness on one hand, and a more cautious approach to continental integration on the other. Interestingly, Botswana stands out as the only country among the top twenty that, despite its advanced ecosystem, remains outside the Malabo community. Interpreting the political or other broader dimensions based on the introduction is beyond the scope of this analysis; therefore, only a brief indication can be provided. The data in Table 3, and the conclusions directly observable from it, demonstrate that cybersecurity decisions in African countries are not driven solely by cyber-threat considerations. General social development and global trends may exert a positive influence on cybersecurity culture and continental cooperation. In this area, natural development would be preferable, rather than progress forced by a major, cross-border cyber incident.

A deeper analysis of the issuance dates and specific mandates of these regulations could provide further insights in subsequent research.

Beyond the institutional landscape, recent data highlight evolving trends in Africa's digital resilience and threat environment. Internet resilience improved between 2022 and 2023, particularly in West, Central, and East Africa, reflecting the expansion of Internet Exchange Points (IXPs) and stronger inter-provider cooperation (Internet Society, 2025).

This progress is reflected in regulatory developments; according to the *ITU Global Cybersecurity Index*, the continent's average score increased by 171% between 2017 and 2024 (Intelpoint, 2024).

The *INTERPOL 2025* report highlights positive global developments, such as enhanced national cybercrime frameworks aligned with the Budapest Convention and expanded digital forensics infrastructure. Increased cyber resilience is also observed through coordinated multi-agency actions and reinforced law enforcement operations, including cross-border intelligence-sharing (INTERPOL, 2025, pp. 26-29).

However, challenges remain significant. Scholarly analysis of cybercrime-related threats underlinse that the growing interplay between online fraud, financial abuse, and dark-web services reflects the emergence of an increasingly organized criminal ecosystem, shaped by persistent structural vulnerabilities (Gulyás, 2025, pp. 11-117, 120-122).

Furthermore, critical constraints to digital transformation include infrastructure gaps, low uptake of digital services, and affordability issues. These are compounded by a lack of digital identification systems and fragmented regulatory environments, which limit the scalability of digital services (World Bank, 2024a).

Finally, the strengthening of CSIRTs remains fundamental to the national cybersecurity ecosystem. Development remains uneven, with some countries maintaining multiple operational teams while others face significant capacity gaps. Addressing these requires targeted investments, enhanced regional cooperation, and sustainable financing models, such as public-private partnerships and the integration of open-source tools (World Bank, 2024b, pp. 5–6, 16–19).

3. Capacity Building Initiatives

As previously discussed, initiatives aimed at defining cybersecurity requirements are already gaining momentum across African nations. This development is essential, as mitigating threats to digital infrastructure cannot be achieved without robust national-level organizational and procedural capabilities. Establishing and maintaining resilient regional and national cybersecurity environments depends not only on legal harmonization but also on targeted capacity development and practical cooperation.

Current threat landscapes illustrate the risks of shortcomings in existing cybersecurity frameworks. According to INTERPOL's 2024 report, cybercrime reached unprecedented levels in Africa in 2023, while the global average number of weekly cyberattacks grew by 23%. The financial impact of cybercrime in Africa was estimated at 10% of GDP in 2021, a figure that has likely increased since. Citing Check Point's 2023 data, the report highlights that African organizations faced ransomware attempts at a weekly rate of 1:15 in 2023, significantly exceeding the global average of 1:31. These campaigns increasingly target critical infrastructure, with the average loss per attack rising to USD 5.13 million in 2023 — a 13% year-on-year increase (INTERPOL, 2024, pp. 10-11, 13).

According to INTERPOL's African Cyberthreat Assessment Report 2025, the most prevalent cybercrimes in 2024 included online scams, ransomware, business email compromise (BEC), and digital sextortion (INTERPOL, 2025, pp. 12 -19). The financial sector remains a primary target for organized criminal groups and financially motivated actors, who increasingly employ "heist-style" operations for high-value thefts, alongside elevated levels of espionage and data exfiltration (Dartnall, 2022, p. 1).

The global evolution of attack vectors further complicates the landscape. Analysis by Palo Alto Networks' Unit 42 indicates a significant increase in the speed of data exfiltration; in a quarter of examined incidents, data was exfiltrated in less than five hours after initial compromise — three times faster than in 2021 (Palo Alto, 2025).

The *ENISA 2025 Threat Landscape* confirms a similar pattern: ransomware, ransomware-as-a-service (RaaS), phishing, and rapid exfiltration are core threats across all regions, indicating that these are global rather than region-specific phenomena. This underscores a shared operational challenge: the shrinking window between compromise and theft makes detection and mitigation increasingly difficult. Consequently, both African and European strategic perspectives point to the same priorities: accelerated detection, strengthened identity and access controls, prioritized patching, and modernized incident-response procedures (ENISA, 2025, pp. 5-10, 16).

Scholarly analysis of cybercrime-related threats underlines that the growing interplay between online fraud, financial abuse, and dark-web services reflects the emergence of an increasingly organized criminal ecosystem, shaped by persistent structural vulnerabilities (Gulyás, 2025, pp. 11-117, 120-122).

The rapid spread of mobile devices and internet services across several African regions has not been accompanied by equally strong and reliable security services or protective mechanisms. This imbalance is reflected in the Central Sahel, where cyber-threat

exposure is amplified by limited defensive capacities and structural vulnerabilities (Vörös Gy, Szulcsányi V, 2025).

To transition from risk to readiness, the following sections examine the key initiatives and institutions providing policy direction, technical support, and incident-response capacity to bolster national cybersecurity frameworks.

3.1. Emerging Frameworks for Capacity Building

The **Accra Call for Cyber Resilient Development** supports the practical implementation of the Malabo Convention's legal framework while strengthening capacity-building mechanisms. Launched at the 2023 Global Conference on Cyber Capacity Building (GC3B), this initiative aims to catalyse global action, positioning cybersecurity as a core element of sustainable development. This voluntary, non-binding framework is built around four strategic pillars: integrating cyber resilience into development strategies, promoting demand-driven capacity building, enhancing coordination among partners, and mobilizing sustainable financing for national programmes (GC3B, 2023).

Analysis demonstrates that the Accra Call effectively bridges the gap between the legal obligations of the Malabo Convention and on-the-ground implementation. It serves as a convening platform for member states, the private sector, financial institutions, and academia, translating high-level policy into technical practice.

This action framework is further complemented by expert coordination mechanisms. The *Global Forum on Cyber Expertise (GFCE) Africa Hub* acts as a central connector, enhancing Africa's influence in international policy fora while linking national priorities to implementation partners. The Hub supports the *Africa Agenda on Cyber Capacity Building (AA-CCB)* and the Cyber Capacity Building Coordination Committee, while hosting communities such as the *Africa Cyber Experts (ACE)*. These structures enable tailored knowledge exchange and multi-stakeholder coordination across governments and civil society (GC3B, 2025, pp. 3, 7, 10, 14-16).

The **Lomé Declaration on Cybersecurity and Cybercrime in Africa** provides a critical political complement to these efforts. By mobilizing high-level commitment, it reinforces national legal frameworks and promotes public–private partnerships, alongside strengthened CERT and Security Operations Centre (SOC) functions. The Declaration fosters regional coordination that operationalizes the practice-oriented delivery model endorsed by the Accra Call (Kamau, 2022).

Finally, the **Africa Agenda on Cyber Capacity Building (AA-CCB)** serves as the overarching continental action framework. Operated by AU level coordination structures, the Agenda focuses on the sustainable strengthening of the continent's cyber capabilities. Beyond supporting the update of national strategies, it enhances the operational readiness of CERT/CSIRT and SOC teams through inclusive skills programmes. Furthermore, the AA-CCB advances the harmonization of regulatory frameworks to improve interoperability and legal certainty, while coordinating resource mobilization for the protection of critical information infrastructure (GFCE, 2023, pp. 2, 8, 10-13).

3.2. Institutional Actors and Capabilities

The Accra Call, the Lomé Declaration, and the Africa Agenda establish an unified strategic direction by setting legal and capacity-building priorities. These frameworks emphasize the urgent need for regulatory harmonization, specialized training, and institutional strengthening. However, the critical challenge lies in translating these high-level mandates into measurable actions and identifying the entities responsible for coordinating their continental implementation.

The **African Union Commission (AUC)**, as the AU's executive body, plays a central role in shaping continental approaches to cybersecurity and digital governance. Its mandate involves advancing Africa's engagement in global cyber-norm processes, supporting negotiations on international cybercrime instruments, and promoting the Malabo Convention as the primary framework for regional security (African Union, 2024).

Furthermore, the AUC works to align national policies with emerging global standards, supports the development of national CERT/CIRTs through the AfricaCERT network, and channels technical assistance for capacity-building efforts (DiploFoundation, 2022).

The **Smart Africa Alliance (SAA)**, a heads-of-state endorsed initiative, accelerates ICT-driven development and digital transformation under the principles of the Smart Africa Manifesto (Smart Africa, n.d. a.).

Guided by its Secretariat, the SAA convenes expert working groups to develop „Blueprints" and „Handbooks" on critical areas such as Digital ID, e-payments, and AI. These technical mechanisms directly support cybersecurity objectives by informing national strategies, harmonizing CERT and SOC capabilities, and monitoring implementation to ensure operational readiness (Smart Africa, n.d. b.).

A significant milestone occurred in December 2024, when the EU and Smart Africa signed Global Gateway agreements to expand secure digital networks and reinforce African-owned data governance (European Commission, 2024).

The **African Centre for Coordination and Research in Cybersecurity (ACCRC)**, based in Lomé, was established in 2022 through a partnership between Togo and the UN Economic Commission for Africa (UNECA). As a direct outcome of the Lomé Declaration, the Centre functions as an Africa-wide cybersecurity intelligence hub. Its objectives include supporting the establishment of national cybersecurity agencies, collaborating with law enforcement, and providing specialized technical research to assist Member States in implementing the Malabo Convention (United Nations, 2022).

Operational coordination is further bolstered by **AfricaCERT**, a regional non-profit platform established in 2012 to support the development and coordination of national CSIRTs across Africa (AfricaCERT, n.d.). AfricaCERT provides national CSIRTs with access to advanced Cyber Threat Intelligence (CTI) platforms and trusted information-sharing mechanisms, facilitating real-time threat monitoring and the early detection of malicious campaigns (Resecurity, 2025).

Finally, the **African Network of Cybersecurity Authorities (ANCA)** serves as a continent-level coordination platform. ANCA's initiatives include the planned establishment of a regional "ANCA CERT," the scaling of the Cybersecurity Innovation Centre (CIC) pilot, and the coordination of regional cyber exercises. Notably, the organization is developing a continent-wide Monitoring & Evaluation (M&E) framework to track progress across member states, a tool intended to clearly distinguish high-level political commitment from tangible on-the-ground results (Smart Africa, 2025).

The following section provides a tabular summary of the key attributes and influence areas of these pivotal organizations.

Institution	Mandate	Primary functions	Geographic scope
African Union Commission (AUC)	Continental executive body responsible for policy coordination, norm promotion and Malabo Convention facilitation	Global norm engagement; Malabo implementation support; regional coordination	Continental
Smart Africa Alliance (SAA)	Accelerate ICT-driven development and enable interoperable national digital strategies	Develop Blueprints/Handbooks; harmonize standards; coordinate partner engagement	Member-state network; continental impact
African Centre for Coordination and Research in Cybersecurity (ACCRC)	Continental wide cybersecurity information and intelligence hub supporting national capacity and strategic research	National capacity building; incident-response support; research & technical assistance	Continental (Lomé)
AfricaCERT	Continental wide platform to support national CSIRTs and facilitate CTI sharing across Africa	Provide CTI platforms; enable trusted information sharing; proactive threat monitoring	Continental
African Network of Cybersecurity Authorities (ANCA)	Continental coordination and regulatory harmonization platform for national cybersecurity authorities	Establish regional ANCA CERT; scale CIC; coordinate exercises and M&E frameworks	Continental (ANCA CERT: regional)

Figure 4: Institutional actors and primary functions.

The overview provided in Figure 4 serves as a functional baseline for understanding the institutional architecture of African cybersecurity. However, it must be emphasized that within such a complex ecosystem, the precise delineation of mandates and responsibilities is of paramount importance.

The presented organizational framework is logically structured, yet it also entails potential coordination risks. For example, continent-wide coordination tasks should be clearly distinguished between the AUC and ANCA. In the case of AfricaCERT and ANCA CERT, continental and regional roles must operate in close alignment, and any form of organizational competition should be consciously avoided.

Prior to the introduction of new mandates or functions, a rigorous analysis should determine which entity is best positioned to assume additional tasks without jeopardizing its core responsibilities or duplicating existing efforts.

Summary and Conclusions

A review of the essential elements presented in this study reveals that Africa's cybersecurity landscape is characterized by complexity rather than simplicity.

The Malabo Convention, adopted over a decade ago as a foundational step, has been followed since 2019 by increasingly targeted national support programmes. The Convention's requirements serve as robust pillars for regional security and remain realistic strategic objectives. However, critical assessments indicate that the development of national capabilities built upon this foundation is proceeding slowly, with effectiveness often hampered by structural constraints.

Some critics demand progress „on all fronts" under the Convention, citing a lack of detailed implementation rules. Based on practical experience, such an expectation is often unrealistic, even in environments where financial and human resources are available. Establishing and sustaining a professional cybersecurity culture requires complex procedural measures, sustained government leadership, and a coherent top-down logic. Chapter two of this study illustrates this reality, providing a pragmatic portrayal of the current maturity levels of national regulatory and organizational frameworks.

From a prospective outlook, an AU level Cybersecurity Strategy — if accompanied by sound political governance, heightened leadership awareness, and targeted support for national authorities — could serve as a transformative development instrument. Success will depend largely on long-term, coordinated support from the AU level bodies described in Chapter Three. With such institutional backing, national authorities can effectively leverage programme resources to build comprehensive cyber-defence frameworks, encompassing legislation, regulatory functions, awareness programmes, and the necessary technical and scientific backbone.

The evidence presented in the study clearly supports the conclusion drawn from the hypothesis that the cybersecurity frameworks of African countries should be strengthened through balanced, strategic-level procedural and organizational measures. As shown in Figure 3, beyond the existence of a national framework, the development of cyber culture is essential for enabling effective cooperation. This can be supported by the continent-level — and not only technical — activities of the actors listed in Figure 4, by the incorporation of feedback, and by the successful mitigation of coordination risks.

AU level programmes and the operation of central organizations must be reinforced by national governmental and political frameworks and decisions.

While a precise forecast for the cybersecurity situation across African countries remains elusive, two actors among the instruments discussed bear a particularly critical responsibility: the **African Union Commission (AUC)**, which must act as a flagship by signalling strategic directions; and the **African Network of Cybersecurity Authorities (ANCA)**, which must provide objective feedback on implementation through its developing Monitoring & Evaluation (M&E) framework.

Providing timely and accurate feedback to decision-makers regarding the status and necessary conditions for implementation would mark a significant milestone in the evolution of the African Union's cybersecurity ecosystem.

Conflicts of Interest

The author declares that he has no competing interest.

Notes on Contributor

Dr. Károly Kassai (Ph.D.) earned his doctorate in military sciences in 2008 at the Miklós Zrínyi National Defense University. His professional work focuses on supporting the full lifecycle of cybersecurity issues in military electronic information systems, including the management of security controls and cooperation with operating bodies, competent authorities, and international partners. He has dealt with training and awareness, system accreditation, and incident management, gaining experience both in system-level tasks and in developing governance-related regulatory frameworks. His scientific interests include reviewing specialist papers and contributing to academic qualification processes.

References

AfricaCERT. (n.d.). African Computer Security Incident Response Teams: Mandate and Core Focus. Retrieved 11 03, 2025, from https://portal.africacert.org/about/

African Researchers Magazine. (2025). The Malabo Convention: Africa's Cybersecurity and Data Protection Framework Explained. Retrieved 12 02, 2025, from https://www.africanresearchers.org/the-malabo-convention-africas-cybersecurity-and-data-protection-framework-explained

African Union. (2000). Constitutive Act of the African Union. Retrieved 10 25, 2025, from https://au.int/sites/default/files/pages/34873-file-constitutiveact_en.pdf

African Union. (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). Retrieved 11 25, 2025, from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union. (2024). Africa at Forefront of Championing Cybersecurity and Digital Transformation in the Global Arena. Retrieved 10 28, 2025, from https://au.int/en/pressreleases/20240816/africa-forefront-championing-cybersecurity-and-digital-transformation

African Union Commission. (2020). The Digital Transformation Strategy for Africa (2020–2030). Retrieved 11 02, 2025, from https://au.int/sites/default/files/documents/38507-doc-DTS_for_Africa_2020-2030_English.pdf

African Union Commission. (2024). African Digital Compact. Retrieved 11 07, 2025, from https://au.int/sites/default/files/documents/44005-doc-EN_African_Digital_Compact_-_July_2024.pdf

Akamo, J. O. (2022). The Malabo Convention and Africa's Cyber Posture. Retrieved 11 22, 2025, from https://ipss-addis.org/wp-content/uploads/2022/11/Policy-Brief-Jesutimilehin-O.-Akamo-.pdf

ALT Advisory. (2022). The Malabo Roadmap: Approaches to promote data protection and data governance in Africa. Retrieved 11 25, 2025, from https://dataprotection.africa/wp-content/uploads/malabo_roadmap_Sept_2022.pdf

Ayalew, Y. E. (2023). The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond? Retrieved 10 27, 2025, from https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/

Bouke M A, A. S. (2023). African Digital Transformation and Cybersecurity: A Critical Analysis of the Malabo Convention. Retrieved 11 20, 2025, from https://arxiv.org/pdf/2307.01966

Dartnall, R. P. (2022). Cyber Threats to the Financial Sector in Africa: An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape. Retrieved 10 25, 2025, from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099830405172214598

Dér, A. (2025). Aspects of Cyber Defence in Africa. *Journal of Central and Eastern European African Studies, 5(1)*. doi:https://doi.org/10.12700/jceeas.2025.5.1.341

DiploFoundation. (2022). Cybersecurity and cybercrime in Africa: Continental and regional policies. Retrieved 11 03, 2025, from https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa/cybersecurity-cybercrime-africa-continental-regio

ENISA. (2025). ENISA Threat Landscape 2025. doi:DOI:102824/1946374

European Commission. (2019). New Africa-Europe Digital Economy Partnership - report of the EU-AU Digital Economy Task Force. Retrieved 10 29, 2025, from https://digital-strategy.ec.europa.eu/en/library/new-africa-europe-digital-economy-partnership-report-eu-au-digital-economy-task-force

European Commission. (2024). EU and Africa strengthen cooperation on digital transformation. Retrieved 11 03, 2024, from https://digital-strategy.ec.europa.eu/en/news/eu-and-africa-strengthen-cooperation-digital-transformation

European Commission. (2024). Global Gateway: EU and Smart Africa strengthen partnership for Africa's digital transformation. Retrieved 11 05, 2025, from https://international-partnerships.ec.europa.eu/news-and-events/news/global-gateway-eu-and-smart-africa-strengthen-partnership-africas-digital-transformation-2024-12-03_en

European Union. (2022). DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 (...).

Forum of Incident Response and Security Teams. (n.d.). FIRST global CSIRT directory. Retrieved 11 20, 2025, from https://www.first.org

GC3B. (2023). The Accra Call for Cyber Resilient Development. Retrieved 10 20, 2025, from https://gc3b.org/the-accra-call-for-cyber-resilient-development/

GC3B. (2025). From Accra to Geneva: Notes from a Travel Journal. Retrieved 11 18, 2025, from https://gc3b.org/wp-content/uploads/2025/09/Accra-Call-Process-Report_Notes-from-a-Travel-Journal-2025.docx-Final.pdf

GFCE. (2023). Africa Agenda on Cyber Capacity Building (AA-CCB). Retrieved 10 12, 2025, from https://gc3b.org/wp-content/uploads/2023/12/Africa-Agenda-Final-Final_Dec-.pdf

Gulyás, A. (2025). Cybercrime and dark web in Africa, 2025. doi:https://doi.org/10.12700/jceeas.2024.4.3-4.278

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. doi:DOI:10.1080/25741292.2023.2199960

Intelpoint. (2024). Africa's cybersecurity score grew from 21 in 2017 to 57 in 2024, a 171% increase. Retrieved 10 25, 2025, from https://intelpoint.co/insights/africas-cybersecurity-score-grew-from-21-in-2017-to-57-in-2024-a-171-increase/

International Telecommunication Union. (2024). Global Cybersecurity Index 2024. Retrieved 11 19, 2025, from https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Internet Society. (2017). Internet Infrastructure Security Guidelines for Africa. Retrieved 10 27, 2025, from https://www.internetsociety.org/wp-content/uploads/2017/08/AfricanInternetInfrastructureSecurityGuidelines_May2017.pdf

Internet Society. (2025). Africa's Internet Resilience Shows Promising Growth, New Internet Society Data Reveals Ahead of Key Conference. Retrieved 11 17, 2025, from https://www.internetsociety.org/news/press-releases/2025/africas-internet-resilience-shows-promising-growth-new-internet-society-data-reveals-ahead-of-key-conference/

INTERPOL. (2024). African Cyberthreat Assessment Report 2024. Retrieved 11 13, 2025, from

https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

INTERPOL. (2025). New INTERPOL report warns of sharp rise in cybercrime in Africa 2025. Retrieved 10 29, 2025, from https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

ITU. (2021). Global Cybersecurity Index 2020. Retrieved 11 20, 2025, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kaaniru, J. (2023). The African Union Convention on Cyber Security and Personal Data Protection: Key Insights. Centre for Intellectual Property and Information Technology Law (CIPIT). Retrieved 10 25, 2025, from https://cipit.org/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/

Kamau, W. (2022). The Lome Declaration on Cybersecurity and Cybercrime in Africa. Retrieved 1029 2025, from https://www.talkafrica.co.ke/the-lome-declaration-on-cybersecurity-and-cybercrime-in-africa/

KPMG Advisory Services. (2022). Advancing cybersecurity with Africa: Study report. Retrieved 10 24, 2025, from https://thegfce.org/wp-content/uploads/2023/05/GFCE-Final-Report-Advancing-Cybersecurity-With-Africa.pdf

Orji, U. J. (2018). The African Union Convention on Cybersecurity: A regional response towards cyber stability? doi:doi.org/10.5817/MUJLT2018-2-1

Palo Alto. (2025). Unit 42. (2025). Global Incident Response Report. Link: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report. Retrieved 11 05, 2025, from https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

Peace and Security Council. (2023). Communiqué PSC/PR/COMM.1171 (2023). Retrieved 11 08, 2025, from https://www.peaceau.org/uploads/1171.comm-en.pdf

Resecurity. (2025). Resecurity and AfricaCERT Forge Strategic Partnership to Advance Cybersecurity Across the African Continent. Retrieved 11 08, 2025, from https://www.businesswire.com/news/home/20250811747007/en/Resecurity-and-AfricaCERT-Forge-Strategic-Partnership-to-Advance-Cybersecurity-Across-the-African-Continent

Smart Africa. (2025). Smart Africa adopts its constitution and 5-year strategy for the African Network of Cybersecurity Authorities (ANCA) to tackle cross-border cybersecurity challenges across the Continent. Retrieved 11 11, 2025, from https://smartafrica.org/smart-africa-adopts-its-constitution-and-5-year-strategy-

for-the-african-network-of-cybersecurity-authorities-anca-to-tackle-cross-border-cybersecurity-challenges-across-the-continent/

Smart Africa. (n.d. a.). Who we are. Retrieved 10 30, 2025, from https://smartafrica.org/who-we-are/

Smart Africa. (n.d. b.). Smart Africa. Retrieved 11 02, 2025, from https://vc4a.com/smart-africa/

TechAfrica News. (2025). Smart Africa strengthens cybersecurity with ANCA's five-year roadmap. Retrieved 11 05, 2025, from https://www.techafricanews.com/2025/02/05/smart-africa-strengthens-cybersecurity-with-ancas-five-year-roadmap

United Nations. (2022). Togo and UN sign MoU to establish the African Cybersecurity Centre. Retrieved 11 14, 2025, from https://africarenewal.un.org/en/magazine/togo-and-un-sign-mou-establish-african-cybersecurity-centre

United Nations Conference on Trade and Development. (n.d.). Data protection and privacy legislation worldwide. Retrieved 11 22, 2025, from https://unctad.org

Vörös Gy, Szulcsányi V. (2025). Cyber Threat Map of the Central Sahel Region, ISSN 2786-1902. *Journal of Central and Eastern European African Studies. Vol. 5 No. 3*. doi:DOI: https://doi.org/10.12700/jceeas.2025.5.3.416

World Bank. (2024a). Digital Transformation Drives Development in Africa. Retrieved 11 17, 2025, from https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

World Bank. (2024b). First responders: The role of computer security incident response teams (CSIRTs) in developing countries: Practitioner note. Retrieved 11 12, 2025, from https://documents1.worldbank.org/curated/en/099060824112023473/pdf/P177852-58c03308-bb90-41d5-a716-3967bd98edc4.pdf