Aspects of Cyber Defence in Africa[1]

Attila Dér[2]

Abstract:

When we think of Africa, cybersecurity is not the first word that comes to mind. But over the last 20 years, Africa's technological development has accelerated dynamically. In an increasing number of African countries, increasingly sophisticated and complex Information and Communications Technology systems are being built. The spread and use of the Internet is an indispensable prerequisite for access to global trade. The rapid growth of smartphones and mobile internet use has enabled many people to connect to the online world for the first time, opening up many new opportunities in trade, education and health services. Unfortunately, however, this development trend also has its drawbacks, such as the growing number of cyber-attacks, which, incidentally, underline the need for and relevance of my research. According to global surveys, the countries most at risk of cyber-attacks are in Africa. The importance of cyber security is therefore being recognised in an increasing number of African countries. In this article, I will discuss the cybersecurity policies of several African states and compare them on the basis of key professional indicators. I will also sketch a general picture of the current situation and some thoughts on future challenges.

Keywords:

Cybersecurity; Africa; Internet Security; IoT; Information and Communications Technology.

[1] DOI: https://doi.org/10.12700/jceeas.2025.5.1.341

[2] PhD Candidate at the Doctoral School for Safety and Security Sciences, Óbuda University, Budapest, Hungary; ORCID: 0009-0008-9547-102X; der.attila@uni-obuda.hu.

1.Introduction

The continent of Africa is culturally, socially and economically very diverse in terms of its size and scope. In addition, there are 54 African states on this vast continent, each with its own unique political system. It is therefore very difficult to compare and unify African countries on any subject. Nothing is more proof of this than the period since the African Union was formed, where there have been fewer successes in unifying African countries on various issues. It will not be any easier to take a unified position in this article, but I will measure an average that is roughly representative of cyber defence on the African continent. I will also highlight a few cases or countries as best or worst practices.

The number of internet users in Africa is growing exponentially, but the continent is lagging behind in cybersecurity, which is a major concern. These concerns have been voiced at several international cybersecurity conferences and various strategies have been developed to address them over the past year or two. Positive practices such as digitisation of government services, biometric identification and facilitating online bank payments have been implemented in several African countries with the support of the African Union. However, these positive developments, while offering a wealth of opportunities, have also brought new challenges in the area of cybersecurity. According to the United Nations Economic Commission for Africa (UNECA), cybercrime is one of the main risks that could threaten Africa's economy. African countries need to take this fact seriously and build their own institutionalised defences against cyber-attackers as soon as possible. Policy consultations should not only be held with some of the more developed African states, but also with the less developed states. It would also be an important task to bring African regions on the margins of technology up to a minimum level of protection. In the remainder of this paper I will explore these issues and propose solutions at the end of the article (Arendse & Van Den Berg, 2024).

2. Current cyber policy in Africa

According to the recently released Cybersecurity Index (CEI), some countries in Africa - Ethiopia - are among the most cybersecurity vulnerable nations in the world. This official survey looked at 108 states, with Afghanistan, Myanmar and Ethiopia among the top three most vulnerable states in terms of cyberattacks.

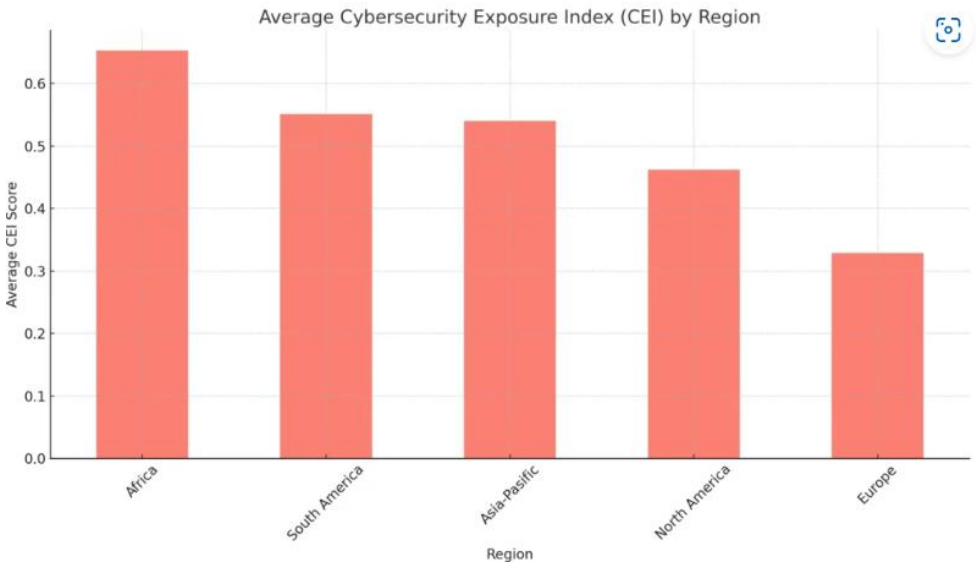

Figure 1: Also shows the extent of the average Cybersecurity Exposure Index (CEI) for Africa. Africa is followed by South America and the best performing region is Europe. As a result, the countries least exposed to attacks are in Europe, such as Finland, Denmark and Luxembourg. Source: Geographical-Insights-Cyber-Security-across-Continents, n.d.

China has become the African continent's number one trading partner. Africa is a major supplier of raw materials to China. There is a large amount of Chinese investment in the African Union, increasing the economic and political weight of the eastern country. In contrast, the European Union and America, given its cultural and historical influence, want to include Africa in their cyber policy holdings. There has already been an attempt by the EU in 2022, but most African states, learning from the past, have been afraid to commit to a platform in the digital space with the West. The current reality, however, is that the growing cyber policy influence of Russia and China in Africa is becoming more powerful through technology investment projects and support for digital sovereignty (Izycki et al., 2023).

In South Africa, there is a growing recognition of the need to respond to cyber-attacks, which are increasing year on year, with a more robust response to their own situation and to that of other African countries. Experts based in South Africa have repeatedly indicated to African Union cyber defence leaders that cyber threat detection should be a core part of the cyber security agenda across Africa. Research shows that these cyber threat detection tools are often neglected or not even used professionally. Yet identifying cyber threats can make a major contribution to stronger cyber security for an organisation or a country. A lot of data can be collected that can later be put to great use by blue teams to prevent or counter attacks. It would be important for organisations to develop a unified cyber threat intelligence model. (Khan et al., 2023)

In the last decade, most countries on the African continent have experienced rapid development in the area of digital culture. African leaders have recognised that their countries cannot remain isolated oases in the ocean of the global world. As a result, the

latest information and communication technologies are being developed in an increasing number of sectors with substantial political and financial support from the state. Internet access is being provided to small and medium-sized enterprises to enable them to compete in international markets with companies of a similar size from other continents. These technologies enable the free flow of information, a key factor for economic development and productivity. The spread of the Internet facilitates communication, innovation and research between companies and educational institutions. However, the advantages of the ever-evolving information and communication technology are accompanied by exponentially growing disadvantages. As a consequence, Africa is also facing an increase in the number and frequency of cyber-attacks. The current situation needs to be assessed through GAP analysis or risk analysis along defined guidelines. Attention must be paid to the continuous improvement of the protection of these systems to maintain their reliability.(African Union, 2024)

3. The rise of computer crime

Terrorist organisations will place increasing importance on developing the technical skills to be able to use these emerging technologies in social media and beyond. Some terrorist groups in East Africa have recognised the potential of television and the internet as a great tool to achieve their goals. It is no coincidence that these organisations are now focusing on the development of information and communication technologies. Unfortunately, the constant online propaganda often has the effect of attracting many new followers to their organisations. It would be hard to imagine to an outsider how purposeful and sophisticated these criminal organisations are in their activities. In order to reach a large part of the African population with this manipulative content, relatively high quality online videos, blogs and topics need to be produced and distributed (Sinkó,G, 2024).

The availability of cheap and reliable internet services in Somalia means that the terrorist group's online content can be accessed by almost anyone, anywhere, at any time. The internet also allows terrorist organisations to exploit the desperation and vulnerability of the African population to their own ends, in order to create a form of chaos (Sinkó,G, 2024).

More than a thousand cybercriminals across Africa have been arrested by Interpol and Afripol as part of Operation Serengeti, which runs from 2 September to 31 October. The operation targeted online fraud and abuse of ransomware and other tools. More than 35,000 victims were identified, and the cases detected caused $193 million (HUF 75 billion) in damages worldwide.(Interpol) Interpol's Secretary General said that cybercrime, which is on the rise on the African continent, should be taken increasingly seriously. He stressed in his speech that unfortunately, law enforcement agencies have not only become aware of the volume of crimes, but also of the sophistication of the fraud, such as bank card fraud affecting the banking sector. Breaking these frauds down by African countries illustrates the trend mentioned above. For example, in Kenya, credit card fraud has increased; in Senegal, an online pyramid scheme involving foreign

fraudsters has taken victims; and huge investment fraud in Nigeria and Cameroon. And in Angola, illegal internet casinos have been shut down (HVG, 2024).

Recently, cyber incidents against African financial institutions have increased rapidly. Attackers have realised that most African countries do not spend enough money on security. Many African countries have outdated Information and Communications Technology on which it is almost impossible to build a modern banking protection system. In many cases, there is a lack of technical background and expertise of IT specialists in applying risk management models to analyse the cyber threats collected (Mbelli & Dwolatzky, 2016).

4. Status of digital regulation

Recently, 37 African countries have adopted national data protection laws. Of these, Nigeria's legislation stands out as being sufficiently robust and widely accepted by society.

Indeed, Nigerian legislation on the protection of personal data has made significant progress in recent years. They have provided a pan-African response to the growing challenges, the protection of fundamental rights and the management of data generated and stored in the context of technological developments. This is the Nigerian Data Protection Act (NDPA), promulgated on 12 June 2023. The NDPA bears some similarities to the emblematic General Data Protection Regulation (GDPR) at European level in terms of specific rights and principles.

Although the 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) is still not in force ten years after its adoption, it is becoming increasingly important for member states of the sub-regional organisation to establish a proper harmonised legal framework, modelled on the European GDPR, to create a safe and attractive digital environment. Firstly, it would facilitate cross-border data exchange, which is essential in sectors such as commerce and finance, as startups such as Wave and Djamo now enable millions of users to transfer money from one country to another using their phones, with the aim of facilitating, securing and protecting the flow of data across borders. Second, with the growth of start-ups and companies in the field of data and cybersecurity, the challenge is to have a clear and coherent legal framework to attract foreign investors and encourage the creation of technology companies. The lack of harmonised legislation is a major violation of the rights and freedoms of citizens in the Economic Community of West African States (ECOWAS) countries and an obstacle to achieving the organisation's objectives. Although such harmonisation seems easy to achieve in theory, it requires strong political will on the part of governments. It would therefore be essential to establish infrastructures and institutions capable of guaranteeing the effective application of the law, following the example of the NDPC and the Federal Competition and Consumer Commission of Nigeria (Olivia ANAGONOU & Sadikou OGOULYI, 2024).

To bring the African Union up to a sufficient level of cyber maturity, the first step is to upgrade the skills and capabilities of the poorest parts of the continent, such as sub-

Saharan Africa. These could be upgrading training, research in security, developing market specific cyber technologies, encouraging women to enter the cyber professions, sharing information on incident management, etc. Without a real alternative, political will and adequate financial backing, the above mentioned ideas will be a failed attempt.

The increased cyber threats on the African continent pose a new challenge to policy makers. Due to their different levels of development, African states can implement and apply the latest technologies in a variety of ways. More specifically, new technologies are being introduced without the country's experts being familiar with the technology or the problems associated with it. This anomaly is also present in cyber defence worldwide, but is a particularly serious problem on the African continent (Abdul-Hakeem, A, 2024).

Strengthening the cyber-security of the African financial system, ensuring the rapid development of digital financial systems and, ultimately, increasing financial inclusion on the continent, would also be a key challenge (Abdul-Hakeem, A, 2024).

Fortunately, more and more regional solutions are now being proposed by stakeholders. A striking example of this is the creation of a joint cyber security and cyber crime strategy for West African countries in the framework of the cooperation between the European Union and ECOWAS. Law enforcement agencies have also established their strategies for the whole of Africa under the leadership of the central body AFRIPOL. Of course, the African Union is also developing its cybersecurity strategy for the whole African continent as part of its defence strategy, with the help of the African Cyber Cyber Expert Community and the Global Forum of Cyber Experts (GFCE).

5. Cybersecurity strategy in Africa

African Union policymakers have realised that there can be no self-made cybersecurity without cross-border international cooperation. A good example is the Malabo Convention, where no effective progress was made on the protection of personal data because the international framework was not in place. Unfortunately, a prerequisite for these African Union pacts would be for each African Member State to have an adequate level of cybersecurity strategy and policy. According to the latest statistics from the UN's International Telecommunication Union, only 20 of Africa's 54 states have a cybersecurity strategy in place, and in most cases, this could be improved. This is problematic because policymakers have nothing to benchmark against and cannot adequately manage economic and public organisations in terms of information technology protection. In Africa, there is no other way to build longer-term cybersecurity than to put in place key legal regulations and strategies, which countries have not yet done.

Some African nations, such as Kenya, South Africa and Senegal, are leading the way with their strategies in place. These countries have already developed their own threat levels, action plans to address them and a system of accountability. I would highlight Nigeria, where a broad social consensus has led to the creation of the Nigerian Cybersecurity Policy and Strategy (NCPS), which is already a good guideline by

international standards. It is through the involvement of a wide range of civil society organisations that the cyber resilience of a country can be truly mapped against foreign intrusions. In this area, African national security institutions are culturally rather closed, almost completely excluding experts from the private sector and other international organisations from shaping their own cyber security strategy. The result is a distorted policy that is not able to effectively coordinate and support the overall IT security of an African state. It is therefore no coincidence that in Kenya, all possible professional organisations with professional competence have been involved in this work. After all, the private sector has much greater and broader expertise, experience and infrastructure than the public institutions themselves. In particular, financial institutions or companies specifically involved in cyber defence, where international cyber security norms, regulations and standards are already in practice. As a consequence, the cybersecurity strategy to be implemented in Nigeria has been integrated relatively smoothly into the public consciousness, as all stakeholders have been consulted on their views and opinions before the drafting process. This fact illustrates what many African countries still need to develop and where their policies need to be positioned within society in order to make the right choices for the future of their state.

The intended outcome of the strategy is that its implementation is in the best interests of all stakeholders. Thus, it is advisable to formulate its style and content in a way that is understandable, so that as wide a section of society as possible can understand and embrace it in their everyday lives. It is also important to mention the rapid development of information technology every year, which poses additional challenges for decision-makers. It is useless to have state-of-the-art target-setting documents (see NCPS) if they are never or only updated every 10 or 20 years. Ideally, the literature suggests that cybersecurity strategies in place should be updated every 5 years to ensure that they do not become obsolete in this rapidly changing dynamic environment. In order to keep their systems secure, they need to continuously respond to the challenges of emerging trends, such as the use of artificial intelligence. A major step forward is the establishment of the Africa Computer Emergency Response Team (AfricaCERT), which will provide strong support and coordination in incident response and investigation in the African Union states. So, the decisions taken now will have a major impact on future cyber security, and will need to be prepared and developed with this in mind and then translated into real life (jeuneafrique, n.d.).

6. Potential cyber attacks in Africa

Failure to regularly investigate cyber risks exposes African small and medium-sized enterprises to potential attacks. The following is a non-exhaustive list of some of the potential cyber-attacks in Africa:Malware: This includes viruses, Trojans and spyware that spread through infected software or websites and cause damage to affected systems.

Denail of Service DoS or Distributed Denial of Service DDoS attacks on critical infrastructures, where control systems can be blocked by inducing large amounts of network traffic. An example of such a typical DoS attack is in power systems, where

intruders disable high-power transformers at substations. The cooling or protection systems of the transformers are shut down and then generated with a fake service request until the transformer heats up to the point where it is completely out of service (Moller et al., 2024).

The Man-in-the-Middle attack exploits the resource-limited computing technology of developing countries. Man-in-the-Middle intrusion techniques allow hackers to manipulate, intercept and steal data from compromised systems by gaining user privileges. Furthermore, the decentralised nature of perimeter networks can also facilitate these forms of attack (Moila & Velempini, 2024).

Exploiting software flaws and vulnerabilities: perpetrators exploit vulnerabilities found in software or operating systems to gain access to the system.

Attacks against supply chains: Trojans or malware planted at suppliers, which can cause serious damage to the customer's infrastructure, or infected updates from suppliers can also pose a high risk!

7. Critical infrastructure situation

The explosion of internet deployment in Africa over the past decade, as discussed in the introduction to this article, has significantly changed the vulnerability and protection of critical infrastructure. It can be observed that the African continent has not developed decades of practical experience in cyber defence, as most African states have not yet started to modernise their information communication technology. In addition, African critical infrastructure has often been outside the attackers' horizon. Clearly, the objective is to gather and implement international best practice lessons learned from the "lagging" experience in Critical Infrastructure Protection (CIP), taking into account local specificities. New models for the protection of mainly state-owned infrastructure should be developed and it is proposed to involve private sector participants. The integrity and interdependence of African systems, both within and across borders, must be taken into account, particularly in view of the current state of affairs. An example is the complex interconnected system of electricity supply, which is an essential element for the economies and populations of the countries' industries to sustain their functioning.

There are analysts who use CIP Assessment Framework (CAF) assessments for risk management of some of Africa's priority facilities. This assessment mechanism must take into account the organisational human resources, educational policies, technology and the regulatory environment of the country. The differences arising from the very different economic and social set-ups of African countries are also well addressed by this CAF framework, which aims to quantify and measure the growth of CIPs. To be more effective, these measures need to be flexible and easy to understand (Musarurwa & Jazri, 2015).

8. Cybersecurity risk analysis

In cyberspace, as in other areas, a rigorous risk assessment must be carried out beforehand to identify threats and define effective security measures to be implemented. There are African countries that use the Expression of Requirements and Identification of Security Objectives (EBIOS) methodology for risk assessment of their critical infrastructures.

The EBIOS risk analysis model consists of five pillars: in pillar one, a complete assessment of the critical system under consideration in terms of risk sources; in pillar two, the objectives to be set are defined; in step three, threat scenarios (strategic and operational) are studied; in step four, operational scenarios are developed to detail the operation of cyber attacks; and finally, in step five, strategic risks and their implementation are summarised.

In most African countries, the following regulatory structure is observed in relation to critical infrastructure information systems security:

- The Cybersecurity and Cybercrime Act
- The Law on the Protection of Personal Data and Children Online
- The Electronic Transactions Act
- Existence of a national internet security strategy or policy
    - A law to establish CERTs (Computer Emergency Response Teams) or a national cybersecurity agency.

So they use risk analysis to identify specific attack paths that malicious red hat hackers can follow depending on the context and environment. Typical practices in African states include higher than average levels of corruption among government employees, where social engineering (attack pathways) can be successfully exploited by intruders. Ultimately, once the analysis has been completed, from the framing and baseline security posture, through the identification of risk sources and targets, to the listing of strategic scenarios and the identification of the most appropriate measures, the process of developing the system's procedures can begin (Cunningham et al., 2018).

9. The importance of education and training

It is important that employees understand the need for cybersecurity and their role in this system.

In Tanzania's study, the government would encourage local IT professionals to develop the country's key information communication technologies rather than foreign specialists. However, the study's survey clearly shows that recent graduates are far from having the skills to properly develop and maintain security-critical software. Unfortunately, IT security skills are not taught in universities, or if they are, they are incomplete and outdated. IT itself, in any field, is a very dynamic and changing environment, so it is essential that it is constantly updated in education and in all aspects of practical life.

The study highlights gaps in university education and suggests further professional training for students or graduates. Lifelong learning and the development of internal

capacities for self-training are also important. Developing an appropriate corporate culture to integrate recent graduates into the world of practice. Many African countries should harmonise the standards and guidelines already laid down by the African Union (Binamungu et al., 2024).

Empowering women to strengthen IT security. Study highlights that attracting women would bring in new talent to organisations running critical industrial systems that have been facing a skills shortage for years. It recommends making education and training as widely available as possible. Girls and boys interested in science should be encouraged and helped from a young age. Employers should help young people who have just graduated with further training and mentoring schemes. Different gender perspectives and mindsets can help a company succeed and innovate effectively in research (Ramonyai et al., 2024).

When training employees, it is worth considering the impact of their behaviour on the security of WiFi and other network systems. Because employees' security behaviours are closely related to subjective norms and levels of cybersecurity awareness. Moreover, training can have the effect of spreading the lessons learned among employees within the organisation (Nguu & Musuva, 2024).

10. Building cyber defences

Government departments, ministries and agencies form a highly sensitive critical infrastructure in a ring of common information communication techniques. The source of the threat is illustrated by the fact that if only one of your institutions is successfully hacked, the others could fall victim. Care must be taken to develop a model that supports not only theoretical training but also simulation training based on interactive real-life situations.

Two-factor authentication and use of biometric identifiers should be made mandatory if possible. This obviously includes the complexity of passwords, where the difficulty of cracking the system depends on the length and combination of the password, apart from the algorithm used to encrypt the password (system dependent) (Tshiamo MOTSHEGWA & Colin WRIGHT, 2018) (Mwangala et al., 2023).

One effective mitigation against DoS and DDoS attacks is GraphQL, a dynamic API data query and management language that can reduce traffic on critical networks by batching queries (Moller et al., 2024).

Firewalls and Intrusion Detection Systems (IDS) do not fully filter out Man-in-the-Middle attacks, so reassuring protection must be complemented by the Cuckoo Search Algorithm (CSA) combined with fine-tuned xDecision Tree technology (Moila & Velempini, 2024).

Access control via intrusion monitoring devices Intrusion detection and prevention systems aim to detect unauthorized access to devices in a protected network. IDPS: Intrusion Detection and Prevention System; IPS: Intrusion Prevention System; IDS: Intrusion Detection System.

Incident response planning is the development of technical procedures, such as a disaster recovery plan, to restore critical IT assets to an appropriate level of service in the event of an emergency.

Blockchain, due to its immutable nature, uses cryptography and consensus algorithms to ensure data integrity, which means that stored data cannot be modified retrospectively. As a consequence, it is worth further developing and more widely deployed in public administrations, banking and other business sectors in African countries, etc (Shozi et al., 2023).

Conclusion

The social, economic and cultural diversity that characterises African states is also reflected to a significant extent in the area of cybersecurity. Some African continents have frontrunners and others have slowly developing societies. The founders of the African Union set out to bridge this gap. They are constantly striving to achieve a single African regulatory framework, where, unfortunately, stakeholders are not always present. Policy consultations should not only be held with some of the more developed African states, but also with the less developed states. It is also important to bring African regions on the margins of technology up to a minimum level of protection.

Even with the most advanced cyber defence solutions, the human factor should not be forgotten. Human intelligence can be the best or the worst defence mechanism, depending on the education and training policy of the organisation. I recommend that staff should be trained as much as possible on the latest cybersecurity theory and practice. And security trainers should run simulations to measure the change in behaviour (Mwangala et al., 2023).

The more underdeveloped sub-Saharan regions lack the basic infrastructures needed to build information communication systems, which are an obstacle to the implementation of innovative alternatives. To this end, it would be an important task to develop a sector-specific action plan for the African continent, taking into account international practices. Furthermore, it would be advisable to introduce blockchain-based guidelines to protect financial services in these countries as soon as possible.

Finally, it would be useful to develop a set of procedures for each continent and country where there are large gaps in these areas. A cybersecurity risk management programme could be developed with the involvement of external, independent experts, including continuous digital monitoring of suppliers (vendors, subcontractors), identification of risks, minimisation of their impact and prevention of their occurrence.

Acknowledgements

Thanks to the research company NextTechnologies and the University of Óbuda's University Research Scholarship Programme, without which the research "Aspects of cyber defence in Africa" would not have been possible.

Conflict of Interest

The authors hereby declare that they have no financial interest in this manuscript.

Notes on Contributor

Attila DÉR is a student at the Doctoral School of Safety Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. He holds a degree in Certified electrical engineering from the Specialization in industrial surveillance and communication systems of Kandó Kálmán Faculty of Electrical Engineers. His research interests include cybersecurity, protection of critical infrastructures in particular energy supply.

References

Abdul-Hakeem, A. (2024). *Cybersecurite-en-afrique-aujourdhui-plus-que-jamais*. Retrieved March 3, 2025 from https://africacenter.org/spotlight/african-lessons-in-cyber-strategy

African Union. (2024). *A global approach on Cybersecurity and Cybercrime in Africa*. Retrieved March 04, 2025 from https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf

Arendse, E., & Berg, C. V. D. (2024, 20-24 May 2024). Exploring the Barriers to Digital Financial Inclusion Amongst Businesses in the Informal Sector. 2024 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569289

Binamungu, L. P., Maro, S., Justo, G., & Ndanguzi, J. (2024, 20-24 May 2024). Assessing Software Safety Knowledge and Skill Gaps in Tanzania. 2024 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569763

Cunningham, P., Cunningham, M., & Institute of Electrical and Electronics Engineers (Eds.). (2018). *2018 IST-Africa Week Conference: 09-11 May 2018. IST-Africa Conference, Piscataway, NJ. IEEE.* Gaborone, Botswana.

Geographical-insights-cyber-security-across-continents. (n.d.). Retrieved March 04, 2025 from https://cyberpandit.org/global-cyber-security-landscape-2023/#8-geographical-insights-cyber-security-across-continents

Heti Világgazdaság (HVG). (November 27, 2024). Interpol-afrika-kiberbűnözes-serengeti-művelet. https://hvg.hu/gazdasag/20241127_interpol-afrika-kiberbunozes-serengeti-muvelet

Izycki, E., Niekerk, B. v., & Ramluckan, T. (2023, 30 May-2 June 2023). Cyber Diplomacy: NATO/EU Engaging with the Global South. 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), DOI: https://doi.org/10.23919/CyCon58705.2023.10182095

Khan, Z. C., Mkhwanazi, T., & Masango, M. (2023, 3-4 Aug. 2023). A Model for Cyber Threat Intelligence for Organisations. 2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), DOI: https://doi.org/10.1109/icABCD59051.2023.10220503

Mbelli, T. M., & Dwolatzky, B. (2016, 25-27 June 2016). Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security. 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), DOI: https://doi.org/10.1109/CSCloud.2016.18

Moila, R. L., & Velempini, M. (2024, 20-24 May 2024). An Optimized Machine Learning Model for the Detection of Man-in-the-Middle Attack in Mobile Edge Computing. 2024 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569231

Moller, A., Makura, S., & Venter, H. (2024, 20-24 May 2024). A Model to Limit Batching Denial of Service Attacks on GraphQL. 2024 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569499

Musarurwa, A., & Jazri, H. (2015, 17-20 May 2015). A proposed framework to measure growth of Critical Information Infrastructure Protection in Africa. 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), DOI: https://doi.org/10.1109/ETNCC.2015.7184813

Mwangala, J., Shava, F. B., & Chitauro, S. (2023, 31 May-2 June 2023). Human Intelligence an Enabler for Cyber Resilience: A Case for Namibian Public Institutions. 2023 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa60249.2023.10187836

Nguu, J. M., & Musuva, P. M. W. (2024, 20-24 May 2024). Determining the Efficacy of Cybersecurity Awareness Programs on Enhancing WiFi Security Behaviour. 2024 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa63983.2024.10569622

Olivia, A., & Sadikou, O. (2024). *La question de la protection des données personnelles en Afrique de l'Ouest à l'occasion du mois de sensibilisation à la cybersécurité.*

Ramonyai, T. M., Mpekoa, N., & Tom, S. (2024, 7-8 March 2024). Cyber security skills development in South Africa: Addressing the Gender Gap in the Industry. 2024 Conference on Information Communications Technology and Society (ICTAS), DOI: https://doi.org/10.1109/ICTAS59620.2024.10507137

Shozi, T., Mtshali, M., Dlamini, S., & Adigun, M. (2023, 31 May-2 June 2023). Blockchain for the Public Service Industry in Sub-Saharan Africa: Analysis of Business Benefits. 2023 IST-Africa Conference (IST-Africa), DOI: https://doi.org/10.23919/IST-Africa60249.2023.10187735

Sinkó, G. (2024). *Afrikai terrorszervezetek internethasználata: Az al-Shabaab tevékenységeinek és képességeinek vizsgálata a harc- és kibertérben. [PhD Thesis]* Biztonságtudományi Doktori Iskola.].

Tshiamo, M., & Colin, W. (2018). Developing a Cyber-infrastructure for Enhancing Regional Collaboration on Education, Research, Science, Technology and Innovation. IST-Africa 2018 Conference. IST-Africa.