HOLISTICA Vol 14, Issue 1, 2023, pp.162-172 DOI:10.2478/hjbpa-2023-0009

UNDERSTANDING THE CHALLENGE OF CYBERSECURITY IN AFRICA: A HOLISTIC ANALYSIS OF SOUTHERN AFRICAN DEVELOPMENT COMMUNITY (SADC) AND FOUNDATION FOR FUTURE RESEARCH

Andreas VASSILAKOS[1]*
Ronald MARTIN[2]

Received: January 2023 | Accepted: April 2023 | Published: June 2023
Please cite this paper as: Vassilakos, A., Martin, R. (2023) Understanding the challenge of cybersecurity in Africa: A holistic analysis of Southern African Development Community (SADC) and foundation for future research, *Holistica Journal of Business and Public Administration,* Vol. 14, Iss. 1, pp.162-172

Abstract

The continuous shift towards a world relying on computing leads to an increase of the potential risk factors that users face while roaming the digital world. The constant technological innovation we are witnessing creates the necessity of developing reliable systems, strategies, and frameworks against nefarious users threatening the security of information and data. Emerging countries begin to face issues related to cyber warfare and security. This study provides insight into the technological risk factors that could potentially delay further development in the technological growth of developing nations, focusing on selected countries in the African continent. The threats against confidentiality, integrity, and availability do not have an impact exclusively on information systems but, to a larger scale, on a region's efforts for innovation. This paper intends to provide the readers a holistic review of the status of cyber security in the context of developing countries, specifically in the African continent and the Southern African Development Community.

Keywords: Information Security, Cyber Security, Cybercrime, Africa, Developing Countries

1. Introduction

In recent years, the impact of cybersecurity and cyberwarfare is becoming immensely important. Humanity is witnessing a shift in the nature of warfare and threats against the security of nations. The increased reliance on electronic means and the innovation in the technological realm provide fodder to threat agents to be creative and focus on targets that might have not yet established strong defense against cyber attacks. The

[1] *Capitol Technology University, Laurel, MD, USA. avassilakos@captechu.edu*
[2] *Capitol Technology University, Laurel, MD, USA. rlmartin1@captechu.edu*
** Corresponding author.*

burden of the imminent threats in the cyber realm is increasingly alarming in the context of developing nations.

Threats in the cyber realm are a global phenomenon, but Africa is especially weak due to issues related to the network and security infrastructure within the continent (INTERPOL, 2021a). The continent's capacity for future growth is proven by the observed digital transformation. Approximately 500 million people have access to the Internet, which is 38% of the continent's population (INTERPOL, 2021a). The constantly expanded infrastructure and digital demand, along with the absence of cybersecurity policy, increases the risk of potential breach at web services (INTERPOL, 2021a). INTERPOL identified online scams, digital extortion, business email compromise, ransomware, and botnets as the top five vectors in the continent (INTERPOL, 2021a). All these vectors can have catastrophic consequences in the national economies of the victim countries.

2. Southern African Development Community

The Southern African Development Community, abbreviated as SADC, is a regional community within the southern African region focusing on economic collaboration. SADC is consisting of the following 16 countries (See Figure 1.): Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic Tanzania, Zambia and Zimbabwe. The aim of SADC is to "to promote sustainable and equitable economic growth and socio-economic development through efficient, productive systems, deeper cooperation and integration, good governance and durable peace and security; so that the region emerges as a competitive and effective player in international relations and the world economy" (SADC, 2022).

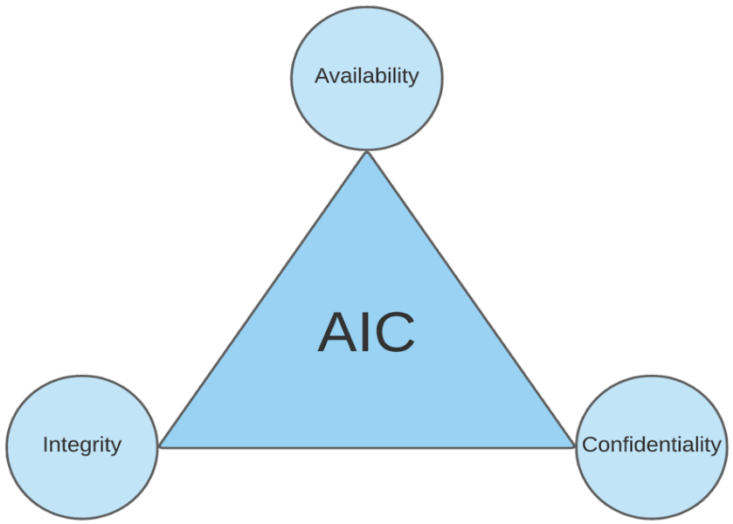
Figure 1 Map of SADC Member States

Source: SADC, 2023

3. Cyber Security

Cybersecurity and its significance is discussed in popular culture, news outlets, and business environments. It is defined as “the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information” (Tips, n.d.). The centerpiece of Cyber and Information Security is the AIC (or CIA) triad (See Figure 2.). AIC is an abbreviation for the three most essential components of security: Availability, Integrity, and Confidentiality. Availability relates to the fact that Hardware, Software, and Data should be present and accessible when the user wants to access them (Conklin, 2018). Integrity is “the security principle that requires that information is not modified except by individuals authorized to do so” (Conklin, 2018). Confidentiality is “The security principle that states that information should not be disclosed to unauthorized individuals'' (Conklin, 2018).

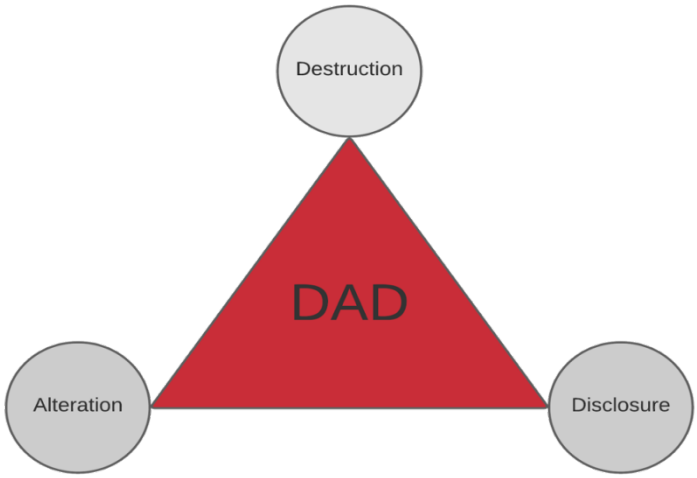
Figure 2 AIC Triad



Source: Authors Design, 2023

In contrast to the AIC triad, which Cyber and Information Security professionals aspire to ensure, the DAD triad describes the consequences of not protecting the AIC triad. The DAD triad stands for Disclosure, Alteration, and Destruction (See Figure 3.).

Figure 3 DAD Triad



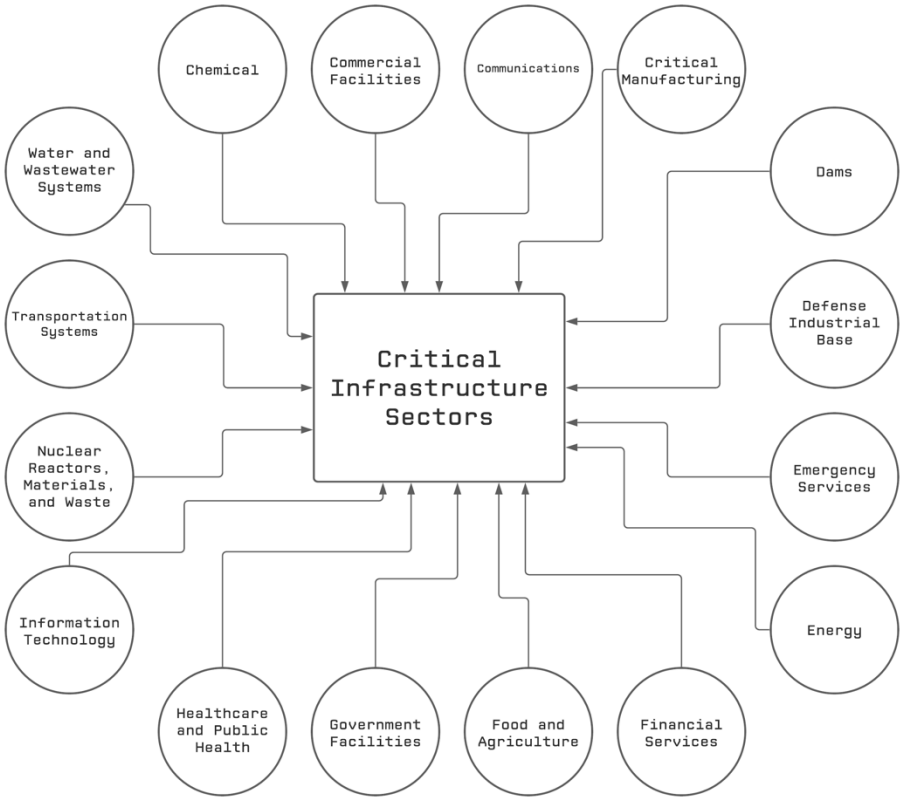
Source: Authors Design, 2023

Cybersecurity professionals are responsible for minimizing any risk associated with the infrastructure and assets they monitor. Risk in the context of information security is defined as "the possibility of damage or harm and the likelihood that damage or harm will be realized" (CISSP glossary, n.d.). The risks that can appear and endanger business systems are a cause for concern and result from threats and vulnerabilities. Threats are circumstances or events that can cause harm to a computing system or infrastructure, and they are a result of vulnerabilities [(Conklin, 2018) and (The Open University, 2016)]. So vulnerabilities, which are flaws that an attacker can exploit to perform unauthorized actions in a system, are to blame for a lot of the issues related to cyber threats (Tips, n.d.). Often, vulnerabilities result from bad or not optimized software engineering practices, which proves the necessity of putting software security at the forefront of program development and prioritizing software security testing.

4. Critical Infrastructure Protection

Currently the Critical Infrastructure in the context of the United States contains the sixteen sectors (See Figure 4.) as described in the Presidential Policy Directive (PPD) 21. In the past, within the Patriot Act that was introduced in 2001, the term "critical infrastructure" was defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".

Figure 4 Critical Infrastructure Sectors in the US Context



Source: Authors Design, 2023

The sixteen Critical Infrastructure Sectors within the PPD 21 include the following: Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; and Healthcare and Public Health. The security of these sectors is increasingly vital in the context of developing nations, as attacks against them can cause hindrance in existing development efforts.

5. Cybercrime in Africa

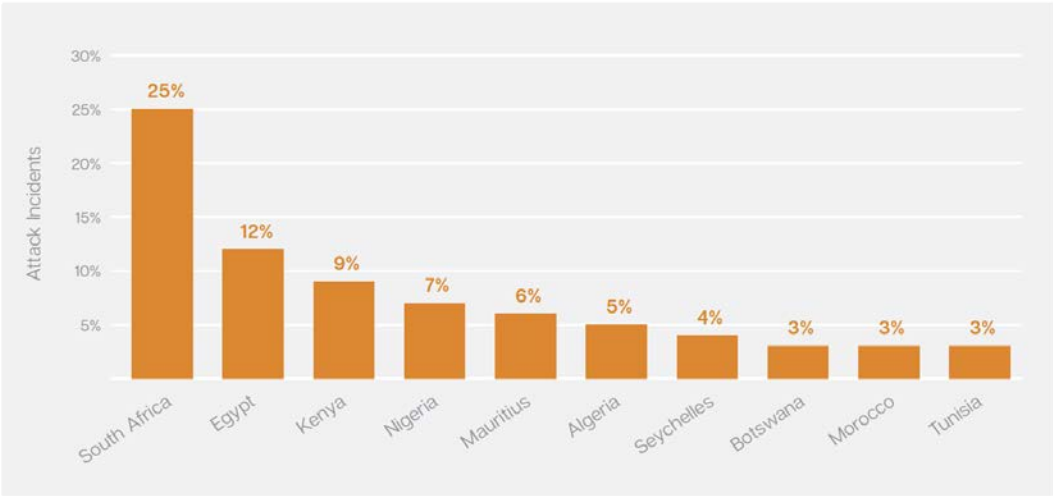
Due to the worldwide and instantaneous connectivity enabled by the technological revolution that has been exhibited for the past years, criminals can expand their agenda on a global scale and their actions do not need to be limited to their geographical location. Developing nations due to their on-going efforts towards digital transformation might not be fully equipped to defend against such attacks. According to Interpol, the African continent is experiencing an increased exhibition of internet-enabled crime due

to the combination of factors such as “the improvement of Internet coverage, the wide availability of cyber-tools and the growing flexibility of cybercriminals” (Interpol, 2020).

Cybercrime is a global phenomenon that includes crimes like identity theft, fraud, and cyber espionage. The continent with the highest growth rate in regards to Internet and telecommunication networks is Africa (INTERPOL, 2021b). The African region is susceptible to nefarious agents in cyberspace because of the vast amount of domains with none or not reliable enough network and security infrastructure to mitigate risks of attack (Heerden, Solms, & Vorster, 2018). It is indicated that the financial impact of cybersecurity-related crimes in Africa is calculated to approximately eight hundred ninety-five (895) million dollars per year. Also, South Africa is placed as the third country in the world with the most victims of cyber attacks (Heerden, Solms, & Vorster, 2018).

According to a report by INTERPOL, the top five threats that are present in the African continent are online scams, digital extortion, business email compromise, ransomware, and botnets (INTERPOL, 2021b). Online scams are described as “fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information” (INTERPOL, 2021b). Digital extortion is considered a situation where “victims are tricked into sharing sexually compromising images which are used for blackmail” (INTERPOL, 2021b). In the case of business email compromise “criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank account” (INTERPOL, 2021b). Ransomware is the criminal act where “cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality” (INTERPOL, 2021b). Finally, botnets are “networks of compromised machines are used as a tool to automate large-scale cyberattacks” (INTERPOL, 2021b).

Figure 5 *Graph for Top 10 Source African Countries for Attacks in 2016*



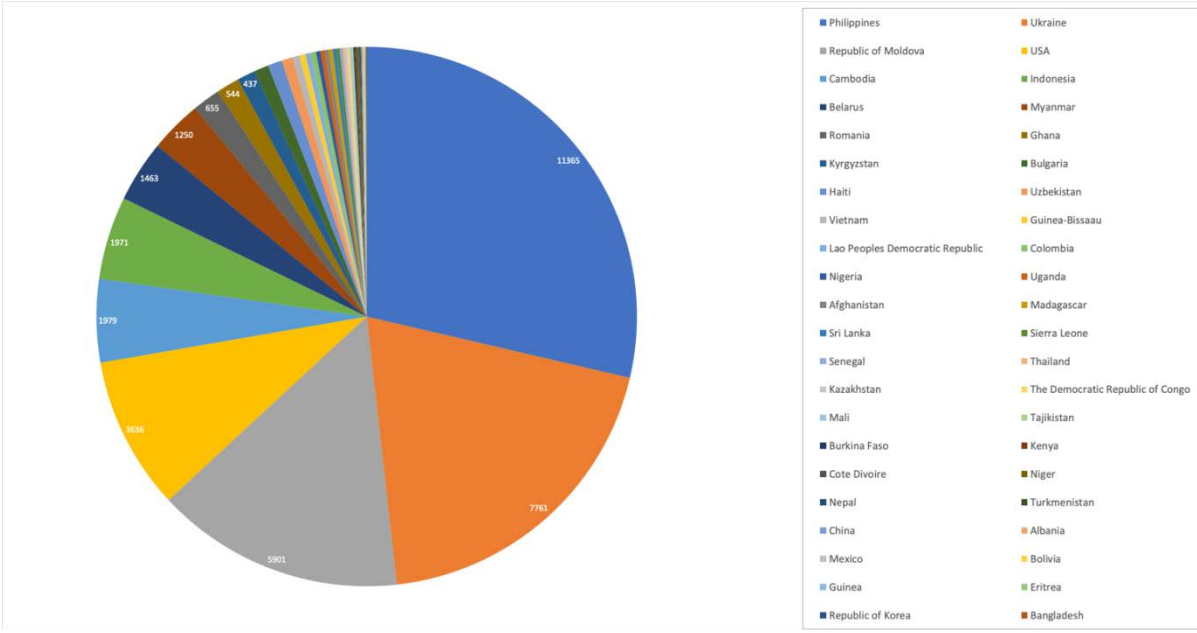
Source: Symantec, 2016

The lack of technical knowledge, the insufficiency regarding appropriate means to monitor and protect nation-wide infrastructure, the limited education, and awareness on cybersecurity, and the lack of initiatives and available frameworks are part of the reason why Africa suffers in the cyberworld (Heerden, Solms, & Vorster, 2018). The hyperconnected modern lifestyle makes any technology user a potential target. Threat agents select the end-users as the target of choice. The ease to be compromised and provide access to sensitive personal information makes them the most vulnerable target (Heerden, Solms, & Vorster, 2018). Humans are the weakest link of information systems, and criminals are always trying to take advantage of this particular vulnerability.

According to Symantec (2016) (See Figure 5.), South Africa was the country with the most occurrences of attacks. South Africa is also the country with the most hacktivists and criminals on the continent (Van Niekerk, 2017). It has been observed that the main impacts of cybercrime in this nation are data exposure and financial theft (Van Niekerk, 2017). Africa, like any other continent in the world, is experiencing a transition to greater exposure to technology, and its population has increased access to the world wide web (Van Niekerk, 2017). Therefore, it is not surprising that the continent is a center of illicit activities. In 2016, political tensions and corruption led to an increase of hacktivism in South Africa, with no demonstrated negative outcome in the national stability and economy (Van Niekerk, 2017). In contrast to hacktivism, espionage is low. The multiple faces cybercrime can exhibit are proved to be another burden in the real hardship the continent battles to facilitate while preparing for the impacts of a scenario where sensitive information is compromised.

Many nefarious users are using the anonymity layer provided by the dark web to hide their criminal acts. The use of digital currency, further complicates combating digital crime. According to Dawson, Vassilakos, Remy, and Setor “Digital currency’s existence, despite the conceptualization of its original form, has been tied to illicit activities in the Deep/Dark Web. Essentially that means that nefarious users have been using this type of money so that they can stay under the radar and hide any trails their actions would potentially leave behind” (Dawson et al., 2021). A part of revenue generated through the Dark Web, is based on human trafficking. After analyzing data provided by the Counter Trafficking Data Collaborative (CTDC), out of the forty four (44) countries of citizenships with the highest count of trafficking victims, 13 countries were identified in the African region (See Figure 6.). The list of countries are Ghana, Guinea-Bissau, Nigeria, Uganda, Madagascar, Sierra Leone, Senegal, Democratic Republic Of Congo, Mali, Burkina Faso, Kenya, Côte D'ivoire, Niger, Guinea, and Eritrea. That is an alarming observation considering the use of technologies to enable human trafficking and obfuscate traces of such activity.

Figure 6 Graph for Top 44 Countries of citizenship in regards to reported victims of trafficking



Source: Authors Design, 2023

6. National Cyber Security Index

The National Cyber Security Index (NCSI) was developed to quantify the preparedness at a global scale of each country against threats in the cyber realm (Ncsi :: Methodology, 2023). The NCSI aims to contribute towards the efforts of fighting cyber crime by the development of their database which is populated by publicly available information (Ncsi :: Methodology, 2023). According to the index's webpage, the initiative's aim is to "…develop a comprehensive cyber security measurement tool that provides accurate and up-to-date public information about national cyber security" (Ncsi :: Methodology, 2023). The index is adjusted using the national cyber security framework as a source for guidance (Ncsi :: Methodology, 2023).

According to NCSI, the index is built following a five-step procedure: "Identification of national level cyber threats, Identification of cyber security measures and capacities, Selection of important and measurable aspects, Development of cyber security indicator, Grouping of cyber security indicators" (Ncsi :: Methodology, 2023). The index is built using evidence from publicly available items, including legal acts, and official documents and webpages and is concentrating their scope on "measurable aspects of cyber security implemented by the central government" in four categories: legislation in force, established units, cooperation formats, and outcomes (Ncsi :: Methodology, 2023). After calculating the "percentage the country received from the maximum value of the indicators", a score is given (Ncsi :: Methodology, 2023). The index also includes a metric called Digital Development Level (DDL), which is the average percentage received

from the maximum value of the ICT Development Index (IDI) and Networked Readiness Index (NRI) for each country (Ncsi :: Methodology, n.d.). The final metric given is Difference, which shows the "relationship between the NCSI score and DDL" (Ncsi :: Methodology, 2023). A positive score means that the country's cybersecurity development is at a similar or better state compared to the digital development experienced in the same country, whereas a negative score means that cybersecurity is not as advanced accordingly (Ncsi :: Methodology, 2023).

Figure 7 Comparison Of Top 10 Source African Countries For Attacks By Symantec Using The Ncsi Index

Source: NCSI, 2023

After comparing the ten countries that were identified in a 2016 report by Symantec by using the NCSI comparison tool (See Figure 7.), it is observed that the country having the best rank is Morocco. Morocco also is the only country that has a rank in the top 50 countries globally. In the rank 50-100 range, seven out of the ten African countries within the Symantec report are identified. The remaining two countries in the Symantec report are ranked in the 100-150 range. It should be noted that the Symantec report was published in 2016, and a great number of developments have occurred since in the cyber security realm.

Figure 8 Comparison Of SADC Countries Using The Ncsi Index

Rank	Country	National Cyber Security Index	Digital development	Difference
58.	Zambia	55.84	29.66	26.18
77.	Mauritius	44.16	53.57	-9.41
89.	South Africa	36.36	49.24	-12.88
105.	Malawi	27.27	23.20	4.07
108.	Tanzania, United Republic of	24.68	26.96	-2.28
114.	Botswana	22.08	41.96	-19.88
133.	Namibia	15.58	37.28	-21.70
130.	Zimbabwe	15.58	28.97	-13.39
135.	Madagascar	12.99	22.80	-9.81
148.	Seychelles	10.39	50.30	-39.91
149.	Angola	9.09	22.69	-13.60
150.	Mozambique	9.09	24.88	-15.79
156.	Congo (Democratic Republic of the)	5.19	18.91	-13.72

Source: NCSI, 2023

After comparing the countries comprising the SADC by using the NCSI comparison tool (See Figure 8.), it is observed that the country having the best rank is Zambia. Zambia, Mauritius, and South Africa are the only countries that have a rank in the top 100 countries globally. In the rank 100-150 range, nine out of the sixteen African countries of SADC are identified. The remaining country, Democratic Republic of Congo, is ranked in the 150-200 range. It should be noted that the NCSI tool did not cover all countries of SADC, as no data were found for Comoros, Eswatini, and Lesotho.

7. Conclusion

The ease of access to technologies is a central component of the modern hyperconnected lifestyle. Cyber attacks are increasing in emerging countries and regions, which adds to the obstacles against the areas' further development. Africa is no exception with many major attacks impacting its populations. South Africa is mentioned as the capital of cybercrime. Nigeria, the African nation with the highest observed growth rate, is facing cybercrime with instances that include the 419 scam (Federal Bureau of Investigation, n.d.). The researchers aimed to set the foundation for future research on cybersecurity in the context of the African continent and countries of the SADC.

8. Conflict of Interest Statement

The research item does not represent the views of the U.S. Government, Department of State, or any other U.S. Government agency. The views and work presented within this item strictly represent the authors' academic work.

References

Counter Trafficking Data Collaborative, Telling Their Stories Through Open Data. (n.d.). Retrieved from https://www.ctdatacollaborative.org/

Critical infrastructure sectors | cisa. (n.d.). Retrieved March 22, 2021, from https://www.cisa.gov/critical-infrastructure-sectors

Dawson, M., Vassilakos, A., Remy, J. L. C., & Setor, T. K. (2021). Illicit Activities Beneath the Surface Web: Investigating Domestic Extremism on Anonymous Social Media Platforms. *HOLISTICA – Journal of Business and Public Administration*, *12*(1), 27–40. https://doi.org/10.2478/hjbpa-2021-0003

Heerden, R. V., Solms, S. V., & Vorster, J. (2018). Major Security Incidents since 2014: An African Perspective. 11.

INTERPOL. (2021a). *AFRICAN CYBERTHREAT ASSESSMENT REPORT INTERPOL'S KEY INSIGHT INTO CYBERCRIME IN AFRICA*.

INTERPOL. (2021b). *INTERPOL report identifies top cyberthreats in Africa*. Retrieved January 22, 2022, from https://www.INTERPOL.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

INTERPOL. (2020). *Online African organized crime from surface to dark web*.

Ncsi: Methodology. (n.d.). Retrieved January 5, 2022, from https://ncsi.ega.ee/methodology/

Ncsi: Ranking. (n.d.). Retrieved April 3, 2022, from https://ncsi.ega.ee/ncsi-index/

Nigeria—The world factbook. (n.d.). Retrieved June 6, 2021, from https://www.cia.gov/the-world-factbook/countries/nigeria/

Federal Bureau of Investigation. (2021) *Nigerian letter or "419" fraud*. Retrieved June 6, 2021, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud

Southern African Development Community. (2023). *Southern African Development Community*. Retrieved January 6, 2023, from https://www.sadc.int/

Symantec (2016). Cyber Security Trends and Government Responses in Africa.

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, (20), 113–132. https://doi.org/10.23962/10539/23573