Cyberterrorism in Africa – Is This the Real Life, Is This Just Fantasy?[1]

Alta Grobbelaar[2]

Abstract:

This paper seeks to examine the relevance of the term 'cyberterrorism' within African spaces. Although the notion of cyberterrorism as a concept is contested by scholars such as Jason Burke and Marc Sageman, the application of the concept in an African context raises a number of concerns. Firstly, rather than focusing on the semantic and conceptual issues only, more attention should be paid to the material implications of such discourses for people and states on the continent who are on the receiving end of such conceptualisation. Discourses regarding fear are always very complex and shape the way in which reality is perceived, understood and how hegemonic power-relations are formed within certain contexts. Secondly, these discourses reflect a Eurocentric bias, because, as visible in the definition used and accepted by US defence analysts, cyberterrorism would refer to "*Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.*". These types of discourses are largely state-centric or government-centric, created to operate in spheres where effective governance varies from what is accepted as such on the African continent. While connectivity and globalization are becoming increasingly important for Africa as a whole, it begs the question whether the term is not more appropriate for highly globalized, technologically advanced contexts of the global North. In contrast with countries in the global North, African countries' limited use and penetration of information technology thus underline the need for a critical (re)examination of the discourses relating to cyberterrorism in the African context. What needs to be established is whether cyberthreats, specifically cyberterrorism, pose a real threat on the continent, or whether the concept has become a platitude or blanket term to describe any form of information-based hostility. The paper questions the application of concepts such as cyberthreats, cyberterrorism and cybersecurity in African-centered approaches.

Keywords:
African security, cybersecurity, cyberterrorism, cyberthreats, terrorism

[1] DOI: https://doi.org/10.59569/jceeas.2023.3.4.197
[2] Lecturer of the University of Free State, Bloemfontein, South Africa; ORCID: https://orcid.org/0000-0003-2246-4810; GrobbelaarA1@ufs.ac.za

1. Introduction

The term "cyberterrorism" might seem like a new threat, a new word, and a new concept in need of examining, defining and explanation. The term was coined in the mid-eighties by research fellow Barry Collin, who defined cyberterrorism as simply as "the convergence of cybernetics and terrorism" (Collin, 1996). Although pinpointing actual events of cyberterrorism throughout history is a difficult task, various scenarios have been imagined where crimes parallel to terrorism – with an added cyber-element – can take place and create mass disruption or even destruction. Cyber-attacks are increasing at an alarming rate around the world (CSIS, 2023) and they are oftentimes linked to the threat of cyberterrorism. As with many contentious terms in politics and international relations, the difficulty does not lie in whether or not the threat is real, but whether or not the threat justifies its own stand-alone field of study, definition and counter-measures.

Mark Pollitt already pondered the validity of cyberterrorism when he wrote whether the threat should be regarded as "fact or fancy" (Pollitt, 1998). He refers to cyberterrorism as "a combination of two great fears of the late 20th century" – random violent events, and new technology. For Pollitt these fears where contextual to the temporal space in which he wrote – the late 90s – and technology was something to be feared because of its ability to carry out actions that used to be done by humans, thus an underlying fear for a loss of control is clear. Thus, this article seeks to examine the validity of cyberterrorism by utilizing the main ideas of the politics of fear, but from an African point of view – a geopolitical landscape that is no stranger to terrorism, but still developing in terms of technological capabilities. Although the temporal and geographical context would differ vastly from Pollitt's in that violence, technology and terrorism are timeless threats, that justify study in as many contexts as possible.

Ongoing understanding of terrorism on a global scale is evolving to include the term 'cyber'. This prefix does not differentiate between different geographic locations, yet the way in which this prefix can impact the well-known threat of terrorism within different contexts will be differentiated across continents, space, and time. To avoid broad generalization regarding the large geographic scope of the research (the Western context and the African context), certain multistate actors and states were strategically selected to provide an overview of terrorism and cyberterrorism discourses in practice.

The article at hand will address the validity and possibility of cyberterrorism in Africa, but before that can be done, a certain understanding of terrorism needs to be achieved. A fundamental problem exists here: the term terrorism has not yet been universally defined, and a myriad of academic works have been published on this contentious issue (Correia, 2022; Ganor, 2002; Margariti, 2019; Saul, 2006; Schmid, 2023; Schmidt, 1984). Thus, this article will start by clarifying a suitable definition or understanding of terrorism within the African context and juxtapose this with possible definitions of cyberterrorism. This will be done by using established definitions as used

by regional and international institutions like the United Nations and the African Union. The comparison of these definitions is important in uncovering how contextually accurate definitions of these threats are, and how different states – all with unique manifestations of various terrorism threats – understand, define, and eventually address the threats of terrorism and cyberterrorism.

As the use of various definitions, their creation, contexts, and applications are central to this study, the use of Critical Discourse Analysis (CDA) will serve as the methodological basis for this study. By using CDA, a possible power imbalance in terms of how discourses regarding cyberterrorism are created will be exposed. As cyberterrorism discourse is more prevalent in a Western context, it is expected that this is where most definitions and discourse regarding cyberterrorism emanate from. The international and regional bodies that address terrorism within this context also have international leverage and discursive advantage, and this may indicate a power imbalance in how African countries apply discourses and guidelines on how to address the threat of cyberterrorism.

Due to the constant change in the nature and appearance of all manifestations of terrorism, and the evolution and impact that the emergence of "cyber" has had on the threat, the use of Critical Discourse Analysis is an important part of this study. A prominent theme in discourse analysis is that specific discourses oftentimes become assumptions that are universally accepted by society – be that a regional, national, or international society. CDA not only studies the texts and words used to describe the phenomenon of terrorism, but also investigates the role of discourse in strengthening or positioning roles in certain power relations. International and multistate institutions, such as the United Nations create resolutions on the prevention of terrorism, to guide member states on how to address threats. With the esteem that these bodies hold, they advocate for a 'safer' and 'better' world (Fairclough, 2013, p. 479), and states across the world are encouraged to participate and support these political and/or economic endeavors, should they want to reap the benefits of this world. This refers to "discursive privilege", as mentioned above, (Thurlow and Jaworski, 2017, p. 246), and in this study it will be examined whether states and multistate actors with more influence in the global arena have discourse privilege over the African context, and how this influences the discourse privilege between the Western context of cyberterrorism and the African context.

2. Discourses and Definitions of Terrorism

There is a steady stream of research done by scholars regards terrorism and its various manifestations across the globe (Archetti, 2015; Giroux, 2016; Nacos, 2016; Waxman, 2011). These analyses increasingly incorporate media and technology and start to lean toward where the proverbial line is crossed into the cyber realm. But, despite this increasing body of knowledge, the prefix "cyber" is pushing researchers and decision

makers to look for even more and better applicable ways to understand the threat of terrorism in a new light. Still the issue remains, how to understand the threat, without the added difficulty of the prefix. It remains open to various interpretations and contextual adaptations. For this study, to gain an encompassing understanding of the minefield of definitions and contextualisations, some definitions of terrorism need to be brought to the fore.

In a report, "Defining Terrorism" Schmid (2023) discusses the difficulty of defining this contested and complex term and addresses the large number of publications that has contributed and continues to contribute to this debate. Schmid employs methods in his report that are very much in line with the principles of CDA, as he starts by examining the histories of terrorism and the term terrorism itself. This indicates contextual relevance of how the term has been employed, and how similarities and differences in its applications can be found. Schmid suggests that rather than defining terrorism, the focus of a definition could be on the terrorist act (Schmid, 2023, p. 10). This approach has already been taken by many Western governments and several conventions and protocols enacted by international organizations like the UN and the AU.

The United Nations International Convention for the Suppression of the Financing of Terrorism defined terrorism in its Article 2.1.b as:

> "Any act intended to cause death of serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act." (United Nations Information Officer, 2002).

This definition is broad in its description of the terrorist act and can be applied in a wide range of contexts, it also does not refer to any specific means of how an act is performed – only to persons affected by an attack – which leaves ample room for this definition to be utilized for cyberterrorism as well. Although no explicit reference is made that the attack is carried out through means of armed conflict, this meaning can be implied, when analysing the position held of "persons not taking active part in the hostilities in a situation of armed conflict". This definition is ambiguous and leaves ample room for interpretation. The United Nations Security Council, in its resolution 1566 of 2004 elaborates on this definition – in terms of the terrorism acts:

> "…criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provide a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act." (United Nations Security Council, 2004).

The definition provided by the United Nations Security Council is an expansion on the first, including the taking of hostages and the creation of a state of fear, or "terror". This is an indication that discourses are adaptable, and that the international organisation that has the discursive privilege to create powerful definitions can take into consideration changing tactics of terrorist organisations. However, both definitions are somewhat limiting in their scope of semantics as they specifically refer to intent – something that legally can only be determined after an attack has taken place, a perpetrator has been apprehended, and intent has been established. Intent – much like motive – can only be determined after the fact, by legal prosecution, after thorough investigation. Thus, eliminating the goal of preemptive counterterrorism since analysis can only happen once attacks have happened, and the perpetrators have been apprehended. The mention of terror in the United Nations Security Council definition of terrorism is a valuable addition to the discourses regarding terrorism, as a state of terror or fear is more easily recognizable than the intent of an attack is determined.

The politics of fear is a valuable consideration here. As Al Gore describes terrorism as "the ultimate misuse of fear for political ends" (Gore, 2004), terrorism, and any use thereof will always have an element of fear added to it. Whether that fear is justified or not is irrelevant to the fear at hand. A threat does not have to have physical consequences for it to generate a response of terror and anxiety from a population – another indication of the power of discourse. Gore continues in his article on the politics of fear stating that disproportionate amounts of fear is created by terrorists in comparison to the actual dangers or threats that they can pose. This research differs with Gore on proportioning fear according to physical or actual danger. On the one hand, it should be contended that states and international organisations alike should be wary and conscious of the possible dangers that terrorists may pose. On the other, by addressing fear – regardless of the consequences or intent of the act – a certain amount of power (discursive or physical) can be taken away from terrorist organisations.

In the same year as the United Nations International Convention for the Suppression of the Financing of Terrorism first draft of their definition, the Organisation for African Unity (later transformed to the African Union) published the Prevention and Combating of Terrorism convention, and defined the terrorism act as:

> "any act which is a violation of the criminal laws of a State Party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number of group of persons or cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated to: 1. Intimidate, put it fear, force, coerce or induce any government, body, institution, the general public or any segment thereof, to do or to abstain from doing any act, or to adopt or abandon a particular standpoint, or to act according to certain principles; or 2. Disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or 3. Create a general insurrection in a state" (Organization of African Unity, 1999).

Similarities can be drawn between the UN definitions of the terrorist act, and that of the OAU. The OAU incorporated a more state-centric approach to their definition, referring to local laws of state parties, freedom, and cultural heritage. This refers to the importance of including contextual knowledge and understanding into international threats. Although the threat of terrorism, and the fear of thereof is something that can be universally understood, it cannot necessarily be universally addressed.

3. Discourses and Definitions on Cyberterrorism

The ideas and possible implications of cyberterrorism were beginning to gain momentum in the late 1990s, during a wave of high-profile terrorist attacks in the United States (the bombing of the World Trade Center in 1993, and the Oklahoma bombing in 1995) as well as attacks on US embassies in Africa (specifically Kenya and Tanzania in 1998). After these events, the Naval Post Graduate School conducted a comprehensive study on "cyberterror" for the US Defence Intelligence Agency. One of the major findings of this research was in line with developments that we see today: "terrorist use of information technology in their support activities does not qualify as cyberterrorism" (Nelson et al., 1999, p. 9). The research and subsequent report proposed a definition of cyberterrorism, limiting cyberterrorism to damage done to digital property. As will be seen, this differs slightly from more modern proposed definitions of cyberterrorism.

> "the unlawful destruction or disruption of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological… As a subset of terrorism, cyberterror involves using information as a weapon, method, or target, to achieve terrorist goals. Cyberterror exists in and beyond cyberspace and includes physical destruction of any device, system of devices, or process with an information component… Acts taken to disrupt, deny service, destroy, and corrupt binary code are thus acts of cyberterror. A characteristic of cyberterror is its ability to leverage inexpensive means to gain disproportionate effects through destruction, denial, deceit, corruption, exploitation, and disruption. Cyberterror can increase the destructiveness, or disruptiveness, of the act by enabling greater target coverage, effect, and efficiency. Cyberterror may augment or support traditional terrorism, or be employed as a distinct form of action in its own right." (Nelson et al., 1999, pp. 9–10).

Existing cyberterrorism discourses and definitions rely on traditional and existing definitions of terrorism, with the added element of the usage of internet technology, as is well illustrated in the text above from the report by Nelson et al. According to Correia (2022, p. 5) attacks can qualify as cyberterrorism if there is a political, social, or economic threat to a group, organization, or country. At the same time, there are

scholars (Futter, 2018; Wall, 2007) who argue that the 'cyber' prefix is nothing more than an umbrella term added on to an already overly complicated term due to the broad spectrum of factors which it tries to cover.

Additionally, there are those scholars (Holt, 2012; Jarvis et al., 2016; Murray et al., 2019) who support the idea that any definition of cyberterrorism should include the behaviour leading up to an act (much like traditional definitions of terrorism and the problem of "intent"), without necessarily resulting in physical disruption or damage – supporting the notion of addressing the fear related to terrorism and cyberterrorism without binding the responses thereto merely to the physical effects or aftermath of these attacks.

The complexity of the cyber-realm further complicates what may and may not qualify as cyberterrorism. Considering discourses on terms like cyber-activism, hacktivism, and cybercrime are used interchangeably, a differentiation of sorts would be needed to draw a clear delineation as to when the intent of online activity was for the purposes of terrorism (as provided in broader and more traditional guidelines) and when not. Academics take different stances on the matter, as seen above, and detecting and investigating cyberterrorist activity would require large amounts of resources, skills and time, something not always readily available within the African context.

Cyberterrorism has the potential to be another very broad topic, and to venture into another decades-long debate on finding definitions would be challenging. Thus, the argument can be made that broader discourses and guidelines could be provided by regional and international organizations – like the United Nations and the African Union – after which states would be in a position of discourse privilege where they could practice their own interpretation of the threat, as it applies within their operational and geographical context.

In terms of proposing a more encompassing academic definition of cyberterrorism, Plotnek and Slay (2020) present a guideline that incorporates modern technology, and the key characteristics present in an array of studied cyber terrorism definitions:

> "Cyberterrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyber-space to cause real world consequences in order to influence fear or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychological, political, economic, ecological, or otherwise that occur outside of cyber space" (Plotnek and Slay, 2020, p. 8).

It can be argued that the motive or intent would serve as the primary mechanism through which regular criminals are distinguished from terrorists. However, the discourses regarding intent or motive would be nearly impossible to quantify, as finding

the scope of these motives is not easy, and this process might render the entire process of trying to create a definition ineffective (Ejeh, 2019).

It is no mere saying that Africa is "a continent on the rise". The African population has grown from 800 million in 2000 to 1.4 billion in 2023, with a median age of 18.8 (Worldometers.info, 2024). Because of this young and growing population, it is no surprise that technological companies would see Africa as a ripe investment opportunity, as these youths are looking for increased global connectivity, social engagement, and expression. Technology adoption in Africa is also rising, and the need for social media and access to mobile ownership (Symantec & African Union Information Society, 2016, p. 7). This opportunity for growth comes with the increased risk of that misuse of growing networks, and advantage being taken from insufficient internet- and cybersecurity, which is not growing at the same pace. As Africa has more than 500 million internet users (placing the region ahead of North America, South America, and the Middle East) (Interpol, 2021), the high demand for online capabilities serves as both an opportunity and a possible threat – should security not be able to keep up with the demand.

Terrorists and terrorist organisations in Africa often make use of information technology for various purposes to advance their ideological causes (Aly et al., 2017; Archetti, 2015; Chiluwa, 2012, 2015; Niglia et al., 2017; Stevens, 2009). These include but are not limited to the spread of propaganda, radicalization, the gathering of information, networking, recruitment, communication, and coordination. According to the previously discussed definitions, the use of technology, internet technology and cyberspace do not equate cyberterrorism. These examples are all known uses of communication technology that have been employed by traditional forms of terrorism for decades. This would indicate that there is a need to differentiate between when internet and cyber activity of terrorists can be deemed "cyberterrorism" and when it forms part of their day-to-day activities.

The UN Counter-Terrorism Centre provides capacity building support to member states, international and regional organizations to help develop and implement effective responses to challenges that the internet and other ICTs provide in countering terrorism. These programmes operate according to UN Security resolutions 2178 (2014) and 2396 (2017). Although these programmes do not classify cyberterrorism as a standalone term, it does express concern over:

> "The use of such technologies for terrorist purposes, including but not limited to artificial intelligence, 3D printing, virtual assets, unmanned aircraft systems, as well as weaponization of commercial drones." (United Nations Office of Counter-Terrorism, 2022)

In 2014 the African Union adopted the Convention on Cybersecurity and personal data protection act (later known as the Malabo Act) (African Union, 2014). This convention was aimed at the establishment of a legal framework for cybersecurity

protection, and to set broad guidelines for the incrimination and repression of cybercrime and related issues. As with the UN guidelines, this convention did not address cyberterrorism directly, as cyberterrorism is viewed as a subsection or subcategory of the broader issue related to cybercrime. In 2019, a more direct stance was taken by the AU as a call was made for more enhanced monitoring of internet activity "in order to combat terrorism activities" (Xinhua, 2019). This call was made during a global conference on counterterrorism in Kenya. To incorporate understanding for the African context, deputy director of the African Center for the Study and Research on Terrorism at the AU specifically called on member states who already adopted and 'domesticated' the existing Malabo Act, to assist their regional partners in improving cybersecurity on the continent – although, by 2019, only two countries have domesticated the Malabo act into their own legislation (Digiwatch Team, 2019).

Just as there is no internationally accepted definition of terrorism, neither is there an accepted definition of cyberterrorism. Various scholars have tried to fill the discursive void by providing differing opinions on what constitutes cyberterrorism, some including the act of using internet technology (Conway, 2006; Goodman et al., 2007; Murray et al., 2019; Wall, 2008), others referring more strongly to the intent to do harm to critical or electronic infrastructure (Cohen, 2014; Goodman et al., 2007; Pollitt, 1998; Wall, 2007). The fact remains that there is no consensus, not amongst scholars, nor among states. This complicates counterterrorism efforts, as terrorist acts within the cyber-realm have even less regard for borders than terrorist acts within geographic regions. An urgent need for the development of minimum standards of security for computer networks remains (Gordon and Ford, 2002), together with the mindful use of surveillance and research methods to share and collect information on terrorist activities – while respecting the growth of internet capacity, user privacy and sovereignty.

4. Is the Fear of Cyberterrorism in Africa Justified?

Although concern about the potential danger posed by cyberterrorism and the use of cyber capabilities by terrorists is grounded in evidence of growing cyberattacks across the globe (CSIS, 2023), the reality of cyberterrorism remains vague. Too often cyberattacks on critical infrastructure of states or institutions could not be classified as cyberterrorism, as it does not meet the poorly defined criteria, and ends up being grouped and classified somewhere in the vast realm of cybercrime. The element of fear, and if the fear is justifiable, is a point that can come under debate in many academic fields. According to the principles of the politics of fear, the threat does not have to manifest into a physical attack for the fear to have a desired effect. In this sense, even the lack of cyberterrorism and cyberterrorism discourses is a possible tool for terrorists – in Africa and beyond.

One of the difficult issues regarding cyberterrorism is whether an act can be deemed cyberterrorism if it results in offline harm. The contention arises in differing between terrorists' everyday use of the internet (dissemination of propaganda, communication, recruitment), and in the coordination of attacks (planning, hacking). Denning purports that a narrow conceptualization of cyberterrorism should include that a cyberattack should be "sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism" (Denning, 2006, p. 6).

This is in accordance with the definitions seen of traditional terrorism, where the concept and idea of fear remains a main element of the discourse. Although the physical effects of cyberterrorism may not be the same as those of traditional terrorism, the effects of the fear and intimidation might be. However, the problem remains that even the expansive definitions of cyberterrorism do not distinguish between cyberterrorism, cybercrime and terrorists' use of the internet, and thus cyberterrorism loses its meaning. One of the definitions of cyberterrorism that lends itself to interpretations and use in the African context is by Dorothy Denning as well:

> "[cyberterrorism is] highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce government or societies in pursuit of goals that are political or social. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction and disruption against digital property" (Denning, 2006, p. 123).

Leading countries with digital capabilities and connectivity in Africa are Kenya with 83% of its population being online, Nigeria with 60% and South Africa with 56% (Interpol, 2021). The risk here arises that in two of these countries significant terrorist organisations are very active (Boko Haram in Nigeria and Al Shabaab in Kenya) and have been known to adapt to innovate and make use of increased technological capabilities (Al Jazeera Staff, 2016; Allen, 2022; Baken and Mantzikos, 2012; Freeman, 2019; SAPA-AFP, 2012). International bodies like the African Union, United Nations and even Interpol have pledged their support towards African countries in improving and developing joint operational frameworks to improve coordinated actions against cybercrimes. In these reports or resolutions, cyberterrorism is hardly the focus, as due to the ambiguity of the discourses surrounding cyberterrorism, it is easier and more encompassing to develop the continent's overall cybersecurity in terms of cybercrime, of which cyberterrorism forms a part – whatever its definition may be.

There is no question that terrorist organisations in Africa use ICT to assist in planning and even carrying out terrorist attacks. A clear example of this is the live Tweeting of the Westgate Mall attack in Kenya in 2013. However, the way ICT was used is not indicative of cyberterrorism, and the attack itself, and others in which ICT was used in planning, does not fall into the scope of what constitutes cyberterrorism –

not even cybercrime in many cases, but merely terrorists' day-to-day usage of the latest technology available to them, to advance their cause. This adds a difficult dimension to cybersecurity in Africa, as Africa's ICT development, and the usage of ICT for these purposes differs from how ICT is used in Western contexts. There is much that can be learnt from the Western contexts, but caution needs to be applied when domesticating policies and guidelines for African use.

Evidence-based policies and developments need to come to the fore in Africa, tailored for the African context of technological development, socio-economic growth – including digital growth – and the nature of terrorist organisations. In Kenya, for example, the Kenyan Terrorism Prevention Act of 2012 has in a sense attempted to prevent the usage of ICT for terrorism, but while doing so has been described as preventing human rights – under the flag of countering terrorism (Horowitz, 2013).

5. Conclusion

To address the question whether cyberterrorism in Africa is "real-life" or "fantasy", a more difficult question of fear needs to be posed: Is fear of the unknown justified, or is fear only justified once the effects thereof are palpable or physical? A real-life cyberterrorism attack is yet to be identified and solidified in the annals of history, yet the fear thereof is ever-present and ever-growing. This fear is justified by increased cybercrime, and the increased vulnerability of international networks to the effects of malicious use of ICT to advance ideological causes of terrorist organisations.

Africa's fast-growing digital capabilities present both an opportunity and a threat. Governments in Africa need to work with multinational and civil society organisations to find suitable alternatives to provide cybersecurity, without encroaching on human rights. It is possible that clearing the field of ambiguous discourses on cybercrime and more specifically on cyberterrorism would assist in this task. If cybercrime is to serve as an umbrella term of which cyberterrorism is a sub-category, then that needs to be clarified, accepted, and addressed accordingly. If not, the concept of cyberterrorism needs re-examining to determine its overall validity in Africa and beyond. Terrorists that are active in African countries like Kenya and Nigeria have proven many times over that they are not only capable of adapting to modern change, but they welcome and embrace it. Thus, the African context of terrorism research needs to adapt to this change as well – all the while applying caution by remaining mindful of the African context of development. Technological development is happening fast – as can be seen in the information provided – but that does not indicate that cyberterrorism is imminent, it merely poses an opportunity to either curb the threat or fear even before it manifests to its fullest potential, or to fall on the wayside an be led by discourses as it trickles from international organisations that do not have access to the lived realities of African nations themselves.

Terrorists all over the world will always aim to make use of the best and most advanced resources at their disposal – be that short wave radios, drones or advanced cyber networks and attacks on information networks. Is this simply another manifestation that will continue to evolve as the threat of terrorism evolves, or will the fear and fantasy of cyberterrorism continue to haunt the dreams of Africans as they yearn for connectivity, online privacy and safety of information?

Conflict of Interest

The author hereby declares that no competing financial interest exists for this manuscript.

Notes on Contributor

Dr. Alta Grobbelaar is a researcher of Terrorism in Africa; Conflict Studies, Critical Discourse Analysis, Cyber Security in Africa, Terrorism Studies, Terrorism and the Media. She has been working as a Lecturer of Political Studies and Governance at the University of Free State Bloemfontein Campus since 2017.

Bibliography

African Union. (2014) African Union Convention on Cyber Security and Personal Data Protection. Available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Accessed: 28 May 2024)

Al Jazeera Staff (2016) 'Q&A: Boko Haram's Changing Tactics', Al Jazeera, 11 February. Available at https://www.aljazeera.com/news/2016/02/qa-boko-haram-changing-tactics-160211045508486.html (Accessed: 28 May 2024)

Allen, K. (2022) 'Weaponised Drones - the Latest Tech Threat to Reach Africa', Institute for Security Studies, 11 October. Available at https://issafrica.org/iss-today/weaponised-drones-the-latest-tech-threat-to-reach-africa (Accessed: 28 May 2024)

Aly, A., Macdonald, S., Jarvis, L., and Chen, T. M. (2017) 'Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization', Studies in Conflict & Terrorism, 40(1), pp. 1–9. DOI: https://doi.org/10.1080/1057610X.2016.1157402, ISSN 1057-610X

Archetti, C. (2015) Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age. Perspectives on Terrorism, 9(1), pp. 49–59. ISSN 2334-3745

Baken, D., and Mantzikos, I. (2012) 'The Cyber Terrorism Shadow Networks in Africa: AQIM and Boko Haram', African Renaissance, 21(1), pp. 27-45. ISSN 1744-2532. Available at https://journals.co.za/content/aa_afren/9/1/EJC120521 (Accessed: 28 May 2024)

Chiluwa, I. (2012) 'Social Media Networks and the Discourse of Resistance: A Sociolinguistic CDA of Biafra Online Discourses', Discourse & Society, 23(3), pp. 217-244. DOI: https://doi.org/10.1177/0957926511433478, ISSN 0957-9265

Chiluwa, I. (2015) 'Radicalist Discourse: A Study of the Stances of Nigeria's Boko Haram and Somalia's Al Shabaab on Twitter', Journal of Multicultural Discourses, 10(2), pp. 214–235. https://doi.org/10.1080/17447143.2015.1041964, ISSN 1744-7143

Cohen, D. (2014) 'Cyber Terrorism: Case studies', in Akhgar, B., Staniforth, A. and Bosco, F. (eds.) Cyber Crime and Cyber Terrorism Investigator's Handbook. Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo: Elsevier, pp. 165–174. https://doi.org/10.1016/B978-0-12-800743-3.00013-X, ISBN 978-0-128-00811-9

Collin, B. (1996) 'The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge', Crime and Justice International, 13(2), pp. 15–18. ISSN 1096-8733

Conway, M. (2006) 'Terrorism and the Internet: New Media—New Threat?', Parliamentary Affairs, 59(2), pp. 283-298. DOI: https://doi.org/10.1093/pa/gsl009, ISSN 0031-2290

CSIS (2023) Significant Cyber Incidents. Centre for Strategic & International Studies. Available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-05/240515_Significant_Cyber_Events.pdf?VersionId=sdxfmetL1DY5GCan1EYIp2vTwsyrgjZw (Accessed: 28 May 2024)

Denning, D. E. (2006) 'A View of Cyberterrorism Five Years Later', in Himma, K. (ed.), Readings in Internet Security: Hacking, Counterhacking, and Society. Boston: Jones and Bartlett Publishers, pp. 1-18. ISBN 978-0-763-73536-4. Available at https://apps.dtic.mil/sti/tr/pdf/ADA484928.pdf (Accessed: 28 May 2024)

Digiwatch Team (2019) 'AU Calls for Cyber Monitoring to Combat Terrorism', Digiwatch, 11 July. Available at https://dig.watch/updates/au-calls-cyber-monitoring-combat-terrorism (Accessed: 28 May 2024)

Fairclough, N. (2013) Critical Discourse Analysis: The Critical Study of Language. London: Routledge. DOI: https://doi.org/10.4324/9781315834368, ISBN 978-1-315-83436-8

Freeman, C. (2019) 'Boko Haram Adopts "Hearts and Minds" Strategy in Nigeria – Inspired by Isil', The Telegraph, 22 May. https://www.telegraph.co.uk/global-

health/terror-and-security/boko-haram-adopts-hearts-minds-strategy-nigeria-inspired-isil/ (Accessed: 28 May 2024)

Futter, A. (2018) '"Cyber" Semantics: Why We Should Retire the Latest Buzzword in Security Studies', Journal of Cyber Policy, 3(2), pp. 201–216. DOI: https://doi.org/10.1080/23738871.2018.1514417, ISSN 2373-8898

Ganor, B. (2002) Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?', Police Practice and Reseach, 3(4), pp. 287–304. DOI https://doi.org/10.1080/1561426022000032060, ISSN 1561-4263

Giroux, H. A. (2016) Beyond the Spectacle of Terrorism Global Uncertainty and the Challenge of the New Media. New York: Routledge. 1st Edition. Radical Imagination Series. DOI: https://doi.org/10.4324/9781315635804, ISBN 978-1-317-26313-5

Goodman, S. E., Kirk, J. C. and Kirk, M. H. (2007) 'Cyberspace as a Medium for Terrorists', Technological Forecasting and Social Change, 74(2), pp. 193–210. https://doi.org/10.1016/j.techfore.2006.07.007, ISSN 1873-5509

Gordon, S. and Ford, R. (2002) 'On the Definition and Classification of Cybercrime', Computers & Security, 21(7), pp. 636–647. https://doi.org/10.1016/S0167-4048(02)01116-1, ISSN 0167-4048

Gore, A. (2004) 'The Politics of Fear', Social Research, 71(4), pp. 779–798. DOI: https://doi.org/10.1353/sor.2004.0040, ISSN 0037-783X

Holt, J. T. (2012) 'Exploring the Intersections of Technology, Crime and Terror', Terrorism and Political Violence, 24(2), pp. 337–354. DOI: https://doi.org/10.1080/09546553.2011.648350, ISSN 0954-6553

Horowitz, J. (2013) Counterterrorism and Human Rights Abuses in Kenya and Uganda: The World Cup Bombing and Beyond. New York: Open Society Foundations. ISBN 978-1-936133-77-2. Available at https://www.justiceinitiative.org/uploads/1b4cef46-0f2f-498a-a16c-cfcefd9897ae/counterterrorism-human-rights-abuses-kenya-uganda-20130403.pdf (Accessed: 28 May 2024)

Interpol (2021) African Cyberthreat Assessment Report. Available at https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf (Accessed: 28 May 2024)

Correia, V. J. (2022) An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom', SN Computer Science, 3(1). DOI: https://doi.org/10.1007/S42979-021-00962-5, ISSN 2661-8907

Jarvis, L., Macdonald, S., and Whiting, A. (2016) 'Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage', Global Society, 30(4), pp. 605–623. DOI: https://doi.org/10.1080/13600826.2016.1158699, ISSN 1360-0826

Margariti, S. (2019) 'Defining International Terrorism to Protect Human Rights in the Context of Counter-Terrorism', Security and Human Rights, 29(1–4). DOI: https://doi.org/10.1163/18750230-02901004, ISSN 1875-0230

Murray, G., Albert, C. D., Davies, K., Griffith, C., Heslen, J., Hunter, L. Y., Jilany-Hyler, N. and Rathan, S. (2019) Toward Creating a New Research Tool: Operationally Defining Cyberterrorism. St. Augusta: OSF Preprints. DOI: https://doi.org/10.31219/osf.io/uk3z7

Nacos, B. L. (2016) Mass-Mediated Terrorism: Mainstream and Digital Media in Terrorism and Counterterrorism. Lenham: Rowman & Littlefield Publishers, Incorporated. ISBN 978-1-4422-4761-1

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., and Gagnon, G. (1999) Cyberterror: Prospects and Implications. Monterey: Center for the Study of Terrorism and Irregular Warfare. Available at https://apps.dtic.mil/sti/pdfs/ADA393147.pdf (Accessed: 28 May 2024)

Niglia, A., Sabaileh, A. Al, and Hammad, A. (eds.) (2017) Countering Terrorism, Preventing Radicalization and Protecting Cultural Heritage: The Role of Human Factors and Technology. Amsterdam, Berlin, Washington DC: IOS Press. NATO Science for Peace and Security Series - E: Human and Societal Dynamics, Vol. 133. ISBN 978-1-61499-754-2

Organization of African Unity. (1999) OAU Convention on the Prevention and Combating of Terrorism. https://au.int/en/treaties/oau-convention-prevention-and-combating-terrorism

Plotnek, J. J., and Slay, J. (2020) 'Cyber Terrorism: A Homogenized Taxonomy', Computers and Security, 102(2), pp. 1-9. DOI: https://doi.org/10.1016/j.cose.2020.102145, ISSN 0167-4048

Pollitt, M. M. (1998) 'Cyberterrorism — Fact or Fancy?', Computer Fraud & Security, 2, pp. 8–10. DOI: https://doi.org/10.1016/S1361-3723(00)87009-8, ISSN 1361-3723

SAPA-AFP (2012) 'Boko Haram "Leader" Issues New Threats in Internet Message', Time Live, 27 January. Available at https://www.timeslive.co.za/news/africa/2012-01-27-boko-haram-leader-issues-new-threats-in-internet-message/ (Accessed: 28 May 2024)

Saul, B. (2006) Defining Terrorism in International Law. Oxford: Oxford University Press. DOI: https://doi.org/10.1093/acprof:oso/9780199535477.001.0001, ISBN 978-0-199-29597-5

Schmid, A. P. (2023) 'Defining Terrorism', International Centre for Counter-Terrorism, March. DOI: https://doi.org/10.19165/2023.3.01, ISSN 2468-0486.

Schmidt, A. P. (1984) Political Terrorism: A Research Guide to Concepts, Theories, Data Bases and Literature. New Brunswick: Transaction Publishers. ISBN 0-444-85602-1

Stevens, T. (2009) 'Regulating the 'Dark Web': How a Two-Fold Approach can Tackle Peer-to-Peer Radicalisation', The RUSI Journal, 154(2), pp. 28–33. https://doi.org/10.1080/03071840902965687, ISSN 0307-1847

Symantec, & African Union Information Society (2016) Cyber Crime Security Trends in Africa. Mountain View: Symantec Corporation World Headquarters. Available https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf (Accessed: 28 May 2024)

Thurlow, C., and Jaworski, A. (2017) 'Introducing Elite Discourse: The Rhetorics of Status, Privilege, and Power', Social Semiotics, 27(3), pp. 243–254. DOI: https://doi.org/10.1080/10350330.2017.1301789, ISSN 1035-0330

United Nations Office of Counter-Terrorism (2022) Cybersecurity and New Technologies. Available at https://www.un.org/counterterrorism/cybersecurity (Accessed: 28 May 2024)

United Nations Information Officer (2002) 'Treaty on Suppression of Financing of Terrorism Comes into Force', United Nations Human Rights Office of the High Commissioner, 8 April. Available at https://www.ohchr.org/en/press-releases/2009/10/treaty-suppression-financing-terrorism-comes-force (Accessed: 28 May 2024)

United Nations Security Council (2004) United Nations Security Council Resolution 1566. Available at https://digitallibrary.un.org/record/532676?ln=en&v=pdf (Accessed: 28 May 2024)

United Nations Security Council (2014) United Nations Security Council Resolution 2178. Available at https://www.un.org/securitycouncil/s/res/2178-%282014%29 (Accessed: 28 May 2024)

United Nations Security Council (2017) United Nations Security Council Resolution 2396. Available at https://www.un.org/securitycouncil/content/sres23962017 (Accessed: 28 May 2024)

Wall, D. S. (2007) Cybercrime: The Transformation of Crime in the Information Age. Cambridge Polity, 2nd Edition. Crime and Society Series. ISBN 0-7456-2736-6

Wall, D. S. (2008) 'Cybercrime and the Culture of Fear: Social Science Fiction (s) and the Production of Knowledge about Cybercrime', Information, Communication & Society, 11(6), pp. 861–884. DOI: https://doi.org/10.1080/13691180802007788, ISSN 1369-118X

Waxman, D. (2011) 'Living with Terror, not Living in Terror: The Impact of Chronic Terrorism on Israeli Society', Perspectives on Terrorism, 5(5–6), pp. 4-26. DOI: https://doi.org/10.4135/9781473917248.n14, ISSN 2334-3745

Worldometers.info (2024) Worldometer: Africa Population Live. Available at https://www.worldometers.info/world-population/africa-population/ (Accessed: 28 May 2024)

Xinhua (2019) 'AU Calls for Online Monitoring to Combat Terrorist Activities', New China, 11 July. Available at http://www.xinhuanet.com/english/2019-07/11/c_138218326.htm (Accessed: 28 May 2024)