Review article
UDK 323.28:004.738.5 (6)
DOI 10.7251/ZNUBL2201257G

CYBERTERRORISM IN AFRICA – EXAGGERATED THREAT OR WORTHY FOE?

Alta Grobbelaar[1]
University of the Free State, South Africa

Abstract: For many decades, the validity of the concept of cyberterrorism has been questioned. Academics have pondered whether this idea should be regarded as "fact or fancy". Over time, development, globalization and connectivity have led one to veer towards the thought that this should be fact. However, various challenges are posed: The standalone concept of terrorism is in itself highly contested, and academics have yet to agree on a single definition of the term. Secondly, almost any form of modern threat can in the current age be studied with the added prefix "cyber-". This raises the question of strategic approaches when combating things like cyberterrorism. The question arises: In how many ways do, and should, these approaches differ from the counterterrorism measures taken against traditional, physical terrorism, and where is a line drawn in the proverbial sand between terrorism, cyberterrorism, crime and cybercrime? In an effort to demarcate the scope and labelling of attacks as cyberterrorism and not necessarily cybercrime, academics have added the element of political motivation and fear to the young and already contested definition of cyberterrorism. This would mean that one of the only aspects differentiating cyberterrorism from terrorism is the use of information technology. This paper questions the validity of the term and threat of cyberterrorism – especially in an African context. With Africa's limited use and penetration of information technology, the question arises whether this is really a new threat, or simply a natural evolution of the age-old threat of terrorism. Terrorists will always use the latest and best technology and means to their disposal; this research paper aims to understand whether that justifies a completely new concept in African security research.

Keywords: *Cyberterrorism; terrorism; African Security; Counterterrorism; cybersecurity*

INTRODUCTION

When aiming to understand the concept of cyberterrorism and eventually minimize the danger and threat thereof, several aspects of the concept need to be understood. Many years ago, Mark Pollitt wrote on Cyberterrorism and whether it was to be fact or fancy (Pollitt, 1998). Take into consideration the context and timeframe in which Pollitt wrote. In his article, he refers to cyberterrorism as a "combination of two the great fears of the late 20th century". This would refer to the fear of random violent events, and the fear of new technology and more specifically, computer technology. For Pollitt, both of these elements capitalize on the fear of the unknown or something that would happen outside of human control, for Pollitt and his contemporaries technology was to be feared because of its ability to do what used to

1 Grobbelaara1@ufs.ac.za

be done by humans – a fear for a loss of control. People believed that technology had the ability to become the master, and humans would be the servant. Luckily for modern research, time is a wise and patient teacher. The politics of fear would still be a relevant method of study when it comes to studying cyberterrorism years after Pollitt's study, but the reasons for fear would be starkly different.

To sufficiently understand cyberterrorism, a certain degree of understanding is needed in terms of terrorism. The concept of terrorism is so disputed and, in some cases, still so ambiguous due to major disagreements on the use of violence for political reasons. Yet, for the purpose of this study, a certain definition, in line with the politics of fear can be used to garner an understanding of terrorism relevant to the context of the research at hand. Because no accepted definition exists, and the legal and academic term "terrorism" is mostly left to the interpretation of states or entities which use the term, the interpretation often changes to the whims of those who use it according to particular interests at particular times (Zeidan, 2004). For the purpose of this study, to minimize ambiguity, a more comprehensive interpretation of AP Schmidt – UN advisor, will be utilized, as it highlights many aspects of terrorism with relevance to the study. The timeframe in which this particular interpretation was published (1983), also provides us with a certain sense of timelessness of the threat of terrorism – be it cyber- or traditional:

"*Terrorism is an anxiety inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby – in contrast to assassination – the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative of symbolic targets) from a target population... Threat- and violence-based communication processes between terrorist (organization), (imperiled) victims, and main targets are used to manipulate the main target (audience[s]), turning it into a target of terror, a target of demands, or a target of attention depending on whether intimidation, coercion, or propaganda is primarily sought.*" (Schmidt, 1983)

Within this definition or interpretation of terrorism, a few concepts become clear. Terrorism has always and will most probably always have a definite element of fear and randomness connected to it. This is in line with Pollitt's idea of the fear of the unknown. When studying terrorism, one cannot disregard the victims or targets of terror – whether they are intentional or not. This is also quite relevant to the idea of cyberterrorism – as will be discussed later in this study. Once a general understanding of terrorism and its connection to fear is established, the element of *cyber-*, and eventually cyberterrorism, needs to be introduced, with the similar aim to create an unambiguous foundation upon which this study can be built to assess the validity of the threat and concept of cyberterrorism.

Cyberterrorism and cyber-attacks are often used as umbrella terms to cover a range of activities taking place via the Internet. The prefix "*cyber-*" originates from ancient Greek and roughly translates to the "the art of steering" (Tabansky, 2011). This is in direct contrast with Pollitt's original idea of fear of something which cannot be controlled, as the basic concept of *cyber-* indicates a form of control. The *cyber-* prefix has become a phrase synonymous with modern activities, to distinguish between traditional and technologically driven methods, in this case: traditional forms of physical terrorism or cyberterrorism. Cyberterrorism definitions are mostly

based on traditional definitions of terrorism, with the added element of internet technology. According to Victoria Correia attacks can qualify as cyberterrorism if there is a political, social or economic threat to a group, organization or country (Correia, 2022). This definition is supported by other scholars who also suggest that activities leading up to the act, not including physical damage or violence should also be included here (Holt, 2012). Both of these viewpoints include the intent and motivations of terror, albeit cyber- or traditional. As technology should form an inherent part of understanding cyberterrorism and in trying to understand if any type of distinction can and should be made between terrorism and cyberterrorism, a more succinct definition to look at the key characteristics of cyberterrorism is also consulted for the purposes of this study:

"Cyberterrorism is the premeditated attack or threat thereof by non-state actors with the intent to use cyberspace 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 cyberspace." (Plotnek, 2021).

This definition goes beyond intent and motivation and looks at the perpetrator, motivation, intent, means, effects and the targets or cyberterrorism – much like the elements included in the definition of terrorism as mentioned by Schmidt. Another valuable definition is put forward by Dorothy Denning, professor of computer science - she presented this quite unambiguous definition to the House Armed Services Committee in 2000:

"Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks 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. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not." (Weimann, 2004)

Denning's definition also considers who cyberterrorism targets, and what would not constitute a cyberterrorist attack. The question that remains is: does the differentiation between terrorism and cyberterrorism constitute an entire concept and topic on its own, or is it merely natural evolution of the terrorism that we have grown to know and fear?

THE POLITICS OF FEAR

The threat of terrorism, and more lately cyberterrorism has grabbed the attention of states and international media houses and the Information Technology (IT) industry. It is a popularized scenario where hackers or computer whizzes would sit in a dark room, behind shining screens and wreak havoc upon the world by typing a few lines of code or pressing a big red button. Most critical infrastructure systems around the world, especially in Western societies are networked through computers, thus the potential threat from cyberterrorism is very alarming. The idea that terrorists could follow hackers' lead and "break the internet" to disable governments,

disarm armies and launch remote attacks embeds an almost tangible fear in even civilians – never mind state decisionmakers, policymakers and security sectors.

As the internet can easily serve as a multiplier for terrorist operations, it is a well-known fact that terrorist organizations use cyberspace as a form of communication, recruitment, to spread propaganda and to coordinate operations. All of the above-mentioned terrorist-activities do not constitute cyberterrorism, as they are simply operational activities of any terrorist organization, and do not refer to an attack, victims of an attack or the use of IT to attack critical infrastructure, as mentioned in the definitions applicable to this study. To this day, a major cyberterrorism incident, with casualties or injuries has not yet occurred, yet the fear of cyberterrorism is quite real. The United States Institute for Peace even uses the term "Cyberterrorism Angst" and refers to a report, published in 1990, that links American fear to terrorism and computers:

"*Increasingly, America depends on computers… Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb*" (Weimann, 2004)

More recent research supports the fear-inducing aspect of cyberterrorism as well. The Chapman University Survey of American Fears ranked the fear of cyberterrorism as seventh among 88 different fears – higher than terror attacks and terrorism (Onat, 2022). The politics of fear features prominently here as people's fear of cyberterrorism evolves around people's consumption of related media content and political rhetoric. Mass media would tend to exaggerate the threat of cyberterrorism due to the newsworthiness and ease with which an audience can relate to the concept of cyberactivity (think back to the analogy of hackers sitting in a dark room, frantically typing code to take over the world). Cybercrimes are more easily related to by the average internet user than traditional forms of terrorism like suicide bombing or radicalized preaching. Here conceptualization once again becomes of paramount importance, as a distinction needs to be made between concepts like "hacktivism" and other cyber activities, and cyberterrorism.

"Hacktivism," a term coined by scholars to describe the marriage of hacking with political activism… "Hacking" is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend not to have political agendas. (Weimann, 2004).

There are some additional political factors to take into consideration when looking at the fear of terrorism, and eventually the fear of cyberterrorism. The political nature of terrorism as a crime, and the political nature of cyberterrorism as a crime both have a distinct influence of ideology and in most cases religion. Understanding of political viewpoints and ideologies is critical when analyzing people's understanding of national security, personal security – or the potential lack thereof. Here a paradigm shift needs to happen where political factors specific to political and individual contexts are taken into consideration. For the purpose of this study, the African viewpoint becomes important. National security, personal security and especially cybersecurity are concepts that are interpreted and understood differently in Africa than in Western parts of the world. Although the *cyber-* prefix is frequently used as a fear-inducing catch-all phrase, the validity of this phrase in Africa should be examined and questioned.

The conjunction of technology – possibly a frightful machine or phenomenon, with terrorism – definitely a frightful phenomenon – guarantees for a fear-inducing weapon to be wielded by those with enough skill and resources to be able to do so effectively. The next question would be, does African terrorist organizations have these skills, and can the *cyber-* prefix be used so freely on the African continent?

CYBERTERRORISM IN AFRICA

Since the 1990's and the end of the Cold War Africa has experienced a strong upward trend in ICT capabilities and technological advancement. Due to availability of markets in terms of a young population, many global investors saw Africa as an investment destination (David, 2020). This has led Africa to undergo a telecommunication revolution for the development of mobile communications within the public and private sectors. According to the International Telecommunication Union database, total mobile penetration has more than doubled in Africa since 2000. Nigeria, South Africa, Uganda, DRC and Cote d'Ivoire have more mobile connections than fixed telephone lines (David, 2020). Yet, as digitalization on the continent increases, one would imagine so too does the potential for attacks by cybercriminals, and of course, cyberterrorists.

Before the concept of cyberterrorism in Africa can be directly addressed, I would first like to provide a bit of context about the rise and various views of Information and Communication technology (ICT). Traditionally ICT is merely seen as an extended term for Information Technology (IT), which serves as an umbrella term for communication and the integration of telecommunication, computers, software, and audio- and visual systems that enable users to gain access to information, store the information and send, receive and manipulate it. Still, the value and requirements of effective ICT differ from sector to sector. In the long term it indicates the importance of cybersecurity and offers a view on the growth in value of the understanding of cyberterrorism and research that can assist in understanding various conceptualizations of ICT.

The minimum requirements of ICT or even cybersecurity will differ for different role players: for a government who reach their citizens through ICT, it is an important tool for governance and the government will want everybody to have access. The activist who wants to bring about ideological change, will see ICT as a convenient instrument for mobilization, but will still attach value to anonymity and privacy. The cybercriminal will possibly conceptualize it as a way to spread a certain view and will mainly want vulnerable audiences to have access. At the same time the law enforcers of an oppressive regime will prefer fewer of its citizens to have access, so that they cannot use ICT to embarrass or challenge the government.

Scholars, researchers and policymakers need to apply caution when it comes to the correlation between Africa's acceptance and advancement of technology on the continent and actual cyberterrorism. As mentioned, no actual cyberterrorist attack has been recorded to date, not in first world countries where technological advancement is commonplace, nor in Africa where security lapses and -loopholes in technological infrastructure might more easily be found and exploited.

Terrorists and violent extremists in Africa make frequent use of information technology for various purposes to advance ideological causes. These include: 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 does not equate cyberterrorism. These examples are all known uses of communication technology that have been employed by traditional forms of terrorism for decades.

A myriad of researchers have conducted studies on the impact of extremist online content on the radicalization process and terrorist behavior. The high and increasing levels of always-on internet access and the easy production and dissemination of violent and radical content may have radicalizing effects, but as Scriven and Gaudette rightly described it, online radicalization does not happen within a vacuum (Scrivens, 2021). In the African context, with the African reliance on community and kinship, it is important to note that although mobile connection has increased over the last few decades, word-of-mouth and societal influences on radicalization and recruitment cannot be discarded for the shiny new toy of cyberspace.

The issue of conceptualization of cybercrime, cyberterrorism and terrorism remains a central one in this study, as terrorists' use of the internet and other ICT networks could simply be categorized as cybercrime. This classification is based on the fact that it indeed contains malicious online acts, and even has a political motive, but might not disrupt essential or critical infrastructure within the states in which these groups operate. Thus, should the contested definitions of cyberterrorism have a certain "check box" process, where would one draw this unclear line between cybercrime, cyberterrorism and traditional terrorism?

The same criminals who would gain financially by targeting critical infrastructure of an African state, might only have a financial motive, but no political motivation – thus would not be labelled cyberterrorists. If other criminals or terrorists then use the same software or systems to target the same critical infrastructure but with the added political or ideological motivation, the label of cyberterrorist would then be applied.

This sheds light on an ongoing debate within cyberterrorism research regarding whether cyberterrorism acts should result in offline consequences, to be regarded as cyberterrorism. This connects to the politics of fear, as Dorothy Denning states that a narrower conceptualization of cyberterrorism specifies that an attack must be "sufficiently destructive of disruptive to generate fear comparable to that from physical acts of terrorism" (Denning, 2006). The destructiveness mentioned in this definition would refer to harms in the physical world, outside of cyberspace, inflicted upon intended or unintended targets as mentioned in the initial definition as mentioned by AP Schmidt earlier in this article. The other side of the cyberterrorism debate is argued by researchers maintaining that the online impact of cyberterrorism is enough to generate fear and intimidation similar to a physical attack by traditional terroristic means. Holt, in this case, argues that "economic hardship produced by a cyberattack, coupled with fear of the likelihood that it may occur again, could be equal to a physical attack" (Holt, 2012).

While keeping in mind that all of these definitions, contestations regarding definitions and debates are purely hypothetical and speculation, expansive definitions are still employed by states on the African continent. These states are hardly capable of addressing the traditional terrorism threat, and are now expected to adapt, advance and employ counter measures to a threat that is not yet understood by even the most developed countries. Without proper differentiation and interna-

tional agreement regarding what exactly the threat is that these nations are facing, creating effective counter-measures would be a near impossible task. There is no distinction between cyberterrorism, cybercrime and terrorists' use of the Internet, and this leads one to accept that cyberterrorism as a concept loses meaning and lacks the rigor to qualify for intense and in-depth academic study.

THE EXISTING DEBATES REGARDING CYBERTERRORISM

Keeping all of this in mind, the debate about the importance of cyberspace for terrorism – especially from an academic perspective – remains at the forefront of the research question of the validity of cyberterrorism as a relevant and necessary concept.

Traditionally the debate is whether the internet and cyberspace serve as substitute for face-to-face platforms for radicalization and operational functions of terrorist groups. Walter Laquer provides valuable insight into this view of the debate and maintains that cyberspace and the possibilities it offers does not translate into what he describes as "real power". It indicates that cyberspace will have a limited effect on terrorism and radicalization. He emphasizes the question mark behind cyberspace by basically claiming that terrorists will always make use of the latest technology available to them, and that audio cassettes were also used in a similar manner to spread propaganda – when that was the latest technological invention (Laqueur, 1999).

Jason Burke, on the other hand, looks at the role of social media in cyberspace and he contends that social media will never replace face-to-face radicalization at a local level (Burke, 2016) (and this is especially relevant to Africa). Burke concedes that the internet and cyberspace do facilitate and ease communication, propaganda, recruitment and donations, but that it cannot be seen as a substitute but rather as an additional and contributing factor.

Then again, Marc Sageman sees the internet and cyberspace as a possible substitute for what he calls "real world" radicalization (Sageman, 2008). He is of the opinion that the internet enables people to create social ties, and gain access to extremist content that changes the entire concept of radicalization. The option of self-radicalization is now offered, where face-to-face contact is not even necessary (the danger here of various interpretations of ideology and propaganda is also increased).

I still don't believe that cyberspace and the potential growth and development of cyberterrorism can be understood as something that takes place either in the "real world" or in cyberspace. I think it is important to understand that as ICT becomes an integral part of our daily lives, a kind of symbiotic relationship develops. Terrorism therefore undergoes a type of transformation and there is a balance to be found between cyberspace and what Sageman describes as the "real world".

If the Westgate Mall attack in Kenya is used as example: ICT was undeniably used to co-ordinate, plan and execute the attack, but the attack cannot be branded as an example of cyberterrorism. Cyberspace played an indisputable part in the execution of the attack, Al Shabaab tweeted throughout how they were progressing through the mall, several hashtags were created in cyberspace for those who wanted to follow the event, and even the Kenyan government used cyberspace to co-ordinate their reaction to the attack (or mis-co-ordinate it, as a result of overuse or misuse of cy-

berspace and the hashtags mentioned). Hence, Sageman's real world and cyberspace co-operate well to create and sustain terrorism in its newest form.

There is a tendency for research to understand the role of the internet and ICT regarding terrorism in a vacuum. It cannot merely be seen as dichotomous, online or offline. The relationship between reality and the virtual world of cyberspace must be understood and examined at a level where the deeper nuance and connections contribute to the existence of cyberterrorism, and traditional terrorism in general. To contribute to this understanding and eventual analysis, contextual and geographical context must be added. Differing countries have different classifications of critical infrastructure, so the targets of terrorism (be it *cyber-* of traditional) would differ depending on contextual aspects like governments, policies, legislature, infrastructure, cultural norms and even age of the population.

CONCLUSION

In the 21st century the sudden growth of the internet has permanently changed society and the nature of modern communication. The internet has become part of our daily lives, and it also plays a growing part in the actions of extremists.

Extremist individuals misuse the internet as a means for advertising, recruiting, propaganda, training and communication. Consequently, it becomes increasingly important to study and understand the factors that influence and fuel violent extremist activities. If the internet, online capacity and online activities of individuals can ease the process of radicalization and promote the spread of extremist activities, it becomes essential for academics, state role players and policy makers to have knowledge thereof.

Even so, there are heated debates among contemporary and historic experts and researchers regarding the relationship between violent extremism and the internet. On the one hand it is argued that the internet plays a more important role than face-to-face interaction in the process of radicalization. On the other hand, it is thought that the role of the internet in the radicalization process is minimal and that it receives too much attention. Luckily the academic way of thought moves past the mere dichotomous dispute and it can be argued that the role of the internet remains complex and contested.

For every user, professional or social, ICT and cybersecurity have a set of requirements and guidelines to adhere to, and that is precisely what makes systematic research and understanding difficult.

ICT can simultaneously be the mediator and challenger of safety and good governance in Africa.

Whatever side of the debate receives the most attention, one thing that cannot be disputed is the fact that the internet and cyberspace are utilized by terror organizations in Africa and across the world to advance their cause. The question remains if this is a new phenomenon, or if this is a natural occurrence within terrorism. As these organizations operate more and more like transnational and even international businesses, it is understandable that any resource that will optimize effectiveness will be utilized. Security awareness and effectivity needs to increase in Africa – this will be one of the key determinants of the success of counterterrorism and counter cyberterrorism initiatives on the continent. It is a development that various role-players on the continent have been working towards for centuries, some with more success

than others, and it is a development that hopefully all key players on the continent will continuously strive to better and improve.

REFERENCES

1. Burke, J. (2016). The age of selfie Jihad: How evolving media technology is changing terrorism. *CTC Sentinel*, 16-22.
2. Correia, V. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom. *Computer Science*, 84.
3. David, O. G. (2020). Information and communication technology penetration level as an impetus for economic growth and development in Africa. *Economic Research*, 1394-1418.
4. Denning, D. E. (2006). A View of Cyberterrorism Five Years Later. In K. Himma, *Readings in Internet Security: Hacking, Counterhacking, and Society* (p. 3). Boston: Jones and Bartlett Publishers.
5. Holt, T. (2012). Exploring the intersections of technology, crime, and terror. *Terror Polit Violence*, 337-54.
6. Laqueur, W. (1987). *Terrorism Reader: A Historical Anthology.* New York: NAL Penguin.
7. Laqueur, W. (1999). *The new terrorism: Fanaticism and the arms of mass destruction.* Oxford: University Press.
8. Onat, I. B. (2022). Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression*.
9. Plotnek, J. S. (2021). Cyber terrorism: a homogenized taxonomy and definition. *Computer Security*, 1-9.
10. Pollitt, M. (1998). Cyberterrorism - fact or fancy? *Computer Fraud & Security*, 8-10.
11. Sageman, M. (2008). The next generation of terror. *Foreign Policy*, 37-42.
12. Schmidt, A. (1983). *Political Terrorism: A Research guide to concepts, theories, data bases and literature.* New Brunswick: Transaction.
13. Scrivens, R. G. (2021). Terrorists' and Violent Extremists' Use of the Internet and
14. Cyberterrorism. In T. Holt, *Crime Online: Causes, Correlates and Context*, pp. 231-262).
15. Caroline Academic Press.
16. Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs*, 75-92.
17. Weimann, G. (2004). *Cyberterrorism: How Real is the threat?* Washington, DC: United States Institute of Peace.
18. Zeidan, S. (2004). Desperately Seeking Definition: The International COmmunity's Quest for Identifying the Specter of Terrorism. *Cornell International Law Journal 36*, 491-492.
19. Moeller, B. (2009). *The Somali Conflict: The Role of External Actors*. Danish Institute for International Studies (DIIS) Report. https://www.econstor.eu/bitstream/10419/59871/1/592906116.pdf
20. Namatovu, R. (2017). *The Stalemate of Peacekeeping Operations in Somalia - United Nations vs African Union. A Masters Dissertation Submitted to the Department of Diplomacy and International Relations*. Lancaster University.
21. Segui, R. (2013). *The Role of the African Union in Somalia: Where to go From Here With the AMISOM Peace Operation*. Policy Paper of the Institut Catala Internacional, April. www.icip.cat
22. Shire, Mohammed I. (2021). Now is the Time to Engage Al-Shabaab. Religious Leaders and Clan Elders can Help. *War on the Rocks*. October 19. https://warontherocks.com/2021/10/now-is-the-time-to-engage-al-shabaab-religious-leaders-and-clan-elders-can-help/
23. Smith, Dillon R. (2016). Realpolitiks and the Deceptive Use of Islamist Narratives in Armed Struggles: The Case of the Northern Mali Conflict. *Critique: A Worldwide Student*

Journal of Politics. Fall. https://pdfs.semanticscholar.org/e502/82ed5ecbdd76d9c77 b981e-b2af8ed89a2e85. pdf?_ga=2.235026049.1853490627.1589133004-149754616.1589133004.
24. Townsend, W. (2012). *Rebuilding a Broken State: Can Elections Resurrect Statehood in Somalia? Consultancy Africa Intelligence*. September 17, 2012, http://www.consultancyafrica.com/index.php?option=com_content&view=article&id=1117:rebuilding-a-broken-state-can-elections-resurrect-statehood-in-somalia&catid=42:electionreflection&Itemid=270
25. Williams, Paul D. (2013). The African Union Mission in Somalia and Civilian Protection Challenges. *International Journal of Security and Development*. August. https://www.stabilityjournal.org/articles/10.5334/sta.bz/
26. Williams, Paul D. (2014) Stabilising Somalia. *The RUSI Journal*. 159(2).
27. Williams, Paul D. (2018). *Fighting for Peace in Somalia: A History and Analysis of the African Union Mission (AMISOM), 2007-2017*. Oxford: Oxford University Press.