The Contribution of Science and Technology in Countering Violent Extremism in Lamu County, Kenya

[1]Brigadier Joseph Kaku Mutua & [2]Colonel (Dr) John Kisilu Reuben (Ph.D.)

[1,2]National Defence University-Kenya

DOI: https://dx.doi.org/10.47772/IJRISS.2023.7883

Received: 09 August 2023; Accepted: 19 August 2023; Published: 14 September 2023

ABSTRACT

This study examines the role of science and technology in countering violent extremism (CVE) in Lamu County, Kenya. The study employed a descriptive research design and mixed-method cross-sectional survey approach, focusing on multi-agency team operations, specifically emphasizing Kenya Defence Forces (KDF) activities in the Boni Forest. The research population comprised key stakeholders and practitioners involved in CVE efforts, totaling 120 officers. A purposive sampling technique ensured diversity within the sample based on participants' expertise, background, functional areas, departments, age, and units within the Kenya Defence Forces. Data collection involved structured questionnaires and key informant interviews for primary and secondary data from books, journals, and operating procedures. Quantitative data analysis employed SPSS for descriptive statistics, while thematic analysis was applied to qualitative data. The study reveals that science and technology have been integral to Kenya's CVE efforts, with the National Counter-Terrorism Center (NCTC) playing a significant role in intelligence gathering and analysis using technology. Collaboration with international agencies allowed sharing of intelligence, aiding the prediction of attacks and identification of areas with prevalent radicalization. Surveillance technologies like drones and CCTV cameras have enhanced monitoring in high-risk areas, leading to effective response measures. Moreover, mobile money transfer systems like M-Pesa are beneficial and susceptible to misuse in financing terrorist activities, emphasizing the importance of partnerships between financial institutions and security agencies. The study recommended integrating science and technology with community engagement, education, and policy initiatives. It underscores the need for a comprehensive community-centered strategy in Lamu County, fostering partnership and trust between the government and local communities. Continuous research, capacity building, and counter-narratives using technology are essential for sustained progress in countering violent extremism. While science and technology offer invaluable tools, collaboration, and holistic approaches remain vital to achieving comprehensive results and maintaining national security.

Keywords: Counter Violent Extremism, Radicalization, Security, Terrorism, Science and Technology

INTRODUCTION

In the age of technology, the war on violent extremism and terror-related activities has been more challenging as terror groups sometimes target critical technological infrastructure in war attacks. However, it is also a time when governments can utilize science and technology to curb violent extremism in many ways. Owen & Richard (2015) opined that since the emergence of the violent extremism concept in the early 2000s, the global terrorist networks and the increasing use of social media and the internet have made violent extremism a more pressing and complex challenge in the 21st century. Researchers across multidisciplinary fields studying the causes of violent behavior acknowledge no single explanation for why individuals turn to violence; however, several risk factors increase the likelihood of violent behavior. They posit that understanding the causes of violent behavior and implementing effective prevention strategies requires a collaborative approach that draws on various scientific fields and involves teamwork between

researchers, practitioners, and policymakers (Hawkins,1995).

In recent years, extremist groups have continued to use technology to spread their message and recruit new members. Research has shown that science and technology can effectively prevent and combat violent extremism by providing innovative solutions for intelligence gathering, analyzing data, and identifying potential threats. A study conducted by the United Nations Development Programme (UNDP) and the Global Center on Cooperative Security (GCCS) investigating the utilization of science and technology in preventing and countering violent extremism established that technology could help identify and track potential terrorists, monitor social media platforms for extremist content, and develop algorithms to predict possible terrorist activity (Hawkins,1995). Furthermore, the study highlighted the importance of collaboration between scientists, researchers, and policymakers to ensure that technology is used effectively to counter violent extremism (The United Nations Global Counter-Terrorism Strategy, n.d)

In another study, the European Union Agency for Law Enforcement Cooperation (EUROPOL) accentuated the significance of technology in countering violent extremism. The EUROPOL study found that extremist groups increasingly used social media platforms to spread propaganda and recruit new members. Conversely, it also established that security agencies could use technology to track and monitor these activities and identify and disrupt terrorist networks. In addition to these studies, various technological solutions, such as algorithms that can detect and remove extremist content from social media platforms, have been developed to counter violent extremism (Twitter usage statistics, n.d). The algorithm uses machine learning to identify patterns in the language and behavior of extremist groups, allowing for the quick and effective removal of such content.

From the African perspective, scholars have examined the potential of science and technology in enhancing CVE efforts in Africa, focusing on social media, big data analytics, and biotechnology (Kakonge, 2017). In their article, "The Use of Science and Technology in Countering Violent Extremism in Africa: Opportunities and Challenges," Mutuma and Kwesi (2018) highlighted the potential of science and technology in enhancing CVE efforts in Africa while also noting the challenges associated with the rapid pace of technological advancement and the need for effective regulation and oversight. These studies underscore the critical role of science and technology in bolstering efforts to prevent and counter violent extremism in Africa. However, they also emphasize the importance of effective regulation, management, and ethical considerations when utilizing these tools. The UN Resolution 2178 (2014) emphasizes the significance of implementing measures adopted under international norms and standards. It acknowledges the necessity of prevention measures in addressing the issue at hand: "Violent extremism, which can be conducive to terrorism," requires collective efforts, "including preventing radicalization, recruitment and mobilization of individuals into terrorist groups and becoming foreign terrorist fighters." The United Nations Security Council calls upon member states to enhance efforts to counter this kind of violence. It recognizes that international cooperation and any measures taken by Member States to prevent and combat terrorism must comply fully with the United Nations Charter.

In Africa, violent extremist organizations (VEOs) operating in various regions have affiliations with well-known global terror groups like Al-Qaeda and ISIS. In particular, there has been a notable increase in activities in West Africa since January 2021, with high-profile attacks occurring in countries such as Burkina Faso, Mali, and Niger. While the Sahel region of West Africa continues to be a significant epicenter of violent extremism and terrorism (VET), the threat has gradually expanded to include the littoral states along the Gulf of Guinea (GoG) (Théroux-Bénoni and Nadia, 2019).

The Somali-based Al-Shabaab militants group abducted the British couple in September 2011 from Kiwayu Safari Village, and the subsequent travel advisories against Kenya severely hampered the tourism industry in the Country. The incident triggered the Kenya Defence Forces (KDF) incursion into Somalia under Operation Linda Nchi (Protect the Country). Consequently, the Al-Shabaab militants formed three elite

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VII Issue VIII August 2023

groups to carry out attacks against the KDF and the AMISOM allies within Somalia. Jaysh Ayman militants, one of the three extremist groups comprised mainly of Kenyan fighters and supported by foreign jihadists, were deployed in Boni forest, Lamu County, to target Kenya's security agencies along the Hindi – Kiunga road, which serves as a vital route for operations by KDF into Somalia. Boni forest extending into Somalia, has gained notoriety as a sanctuary for the extremists. They have been utilizing it as a base to launch attacks into Lamu and the neighboring counties of Garissa and Tana River. The forest area became a hotbed of violent extremist activity by the Al-Shabaab group, leading to a significant threat to national security in Kenya. The KDF deployed in Lamu County as part of the multi-agency team to protect the area and conduct counter-terrorism operations against Al-Shabaab.

The forest's juggling characteristics and the elusive nature of the militants pose a significant strain on the security teams. Despite the efforts of the security forces, the militants have persisted in carrying out sporadic attacks in the region. The persistent insecurity has led to concerns among the local communities regarding their safety. The lack of a complete solution led to the scholarly quest to establish whether science and technology can assist the Kenya Defence Forces in countering violent extremism in the Boni forest.

THEORETICAL FRAMEWORK

The study was anchored on institutional theory, which emphasizes that the institutional environment significantly influences the development of formal structures within organizations, often surpassing the impact of market pressures. According to this perspective, organizations that are early adopters of innovative structures that enhance technical efficiency will likely gain legitimacy within their environment. As these innovative structures become increasingly accepted and endorsed, there comes a point where not adopting them is viewed as "irrational and negligent" or even becomes a legal requirement. In essence, the institutional environment shapes the norms, values, and expectations organizations must adhere to gain legitimacy and maintain their standing within the broader social and regulatory context. This institutional pressure can drive organizations to adopt new structures, practices, and technologies perceived as more efficient or effective. By doing so, organizations align themselves with the prevailing institutional norms, which can confer legitimacy and enhance their reputation among stakeholders.

The process of institutionalization involves not only formalizing these innovative structures within an organization but also ensuring their broader acceptance and recognition within the institutional environment. Once a particular structure or practice becomes widely legitimized, it becomes increasingly difficult for organizations to resist its adoption without facing potential penalties or being seen as deviant or outdated. According to Sandre, applying technological innovation to activities of law enforcement has brought about a revolution in the ability of police to, on the one hand, respond to real-time crime and, on the other hand, to anticipate and establish problems, ascertain their cause and create strategic plans that improve an agency's crime prevention (Sandre, 2015) According to Pelling, for security institutions to keep crimes such as hacking, armed robbery, kidnapping, rape, murder, arson, bomb attacks, and burglary, among others, in check, there is a need to adopt both hard and soft technological use (Pelling, 2015).

RESEARCH METHODOLOGY

The study employed a descriptive research design and a mixed-method cross-sectional survey approach to investigate multi-agency team operations in Lamu County, focusing on the Kenya Defence Forces (KDF) activities in the Boni Forest. The research population included key stakeholders and practitioners involved in countering violent extremism (CVE) in Kenya and Somalia, such as Kenya Police, National Intelligence Service, civil societies, intelligence agents, terrorist victims, and Anti-Terrorism Police Unite, United States Agency for International Development, United Nations agencies, Kenya Defence Forces and other security experts, totaling 120 officers. The study sample size was determined through Krejcie & Morgan's (1970)

formula, which states that for a population of 120, a sample of 92 is sufficiently representative. A purposive sampling technique was utilized to ensure diversity within the sample, selecting participants based on their expertise, background, functional areas, departments, age, and units within the Kenya Defence Forces. Data was collected through structured questionnaires and key informant interviews for primary data, and secondary data was obtained from books, journals, and standing operating procedures. Quantitative data was analyzed using SPSS, with descriptive statistics such as frequencies and percentages derived from coded questionnaire responses. For qualitative data, thematic analysis was applied to identify patterns and meaningful responses related to the research questions.Top of Form

FINDINGS

Application of Science and Technology in Counter-Violent Extremism in Lamu

The study sought to establish how technology was applied to counter violent extremism in Lamu County, Kenya. The researcher identified various mechanisms through which technology was utilized in CVE. The findings are shown in Table 4.1.

Table 4.1 Counter-Violent Extremism Mechanism

Strategies	**Frequency**	**Percent**
Establishment and Strengthening Capacity of the National Counter-Terrorism Center (NCTC) as the focal point	28	30.4%
Sensitization and Awareness Programs	24	26.1%
Increased surveillance along and within the Boni forest	24	26.1%
Nyumba Kumi Policing	16	17.4%
Total	**92**	**100.0%**

(Source: Researcher 2023)

DISCUSSIONS

Establishment and Strengthening Capacity of the National Counter-Terrorism Center (NCTC) as the focal point

When asked whether science and technology have been used in countering violent extremism in Kenya, the respondents acknowledged that science and technology had been used in CVE in Kenya. In Table 4.1, the top strategy was establishing the National Counter-Terrorism Center (NCTC), utilizing technology for intelligence gathering and analysis to prevent attacks, as supported by 28 (30.4%) respondents. The findings reflected the Government's commitment to the war against terror through the utilization of technology and a multi-agency approach.

According to the National Counter Terrorism Centre website, the National Counter Terrorism Center (NCTC) is a multi-agency institution established by the Prevention of Terrorism Act to strengthen the coordination of counter-terrorism activities. "The organization was created in 2004 through a cabinet decision in response to developing a national counter-terrorism strategy". In 2014, "through the Security Amendment Act 2014, NCTC became legally established and mandated to coordinate national counter-terrorism initiatives, conduct sensitization of Kenyans on countering terrorism and Violent extremism, initiate measures to counter radicalization and foster de-radicalization and also facilitate training on terrorism prevention, among others."

The National Counter-Terrorism Center (NCTC) works closely with various international agencies in sharing data and information that could be helpful in CVE efforts not only in Lamu County but also in various parts of the Country. According to the NCTC website, the Centre collaborates with Interpol terrorism, various United Nations agencies that focus on CVE, the Global Counter-terrorism Forum, African Union and its various CVE affiliates, Global Terrorism Database, among other agencies. Through these collaborations, the National Counter-Terrorism Center (NCTC) employs the use of technology in sharing intelligence with other global organizations and, as such, can predict attacks, identify areas where radicalization is common and intercept online information that could lead to radicalization, and as such work towards CVE. Additionally, the multi-agency approach has enabled capacity building for stakeholders and officers from various security agencies who can share their experiences, expertise, and technical know-how to strengthen each other, enabling more effective responses to Violent Extremists(VE) threats in Kenya.

The findings agreed with Kivunzi and Nzau (2018), who opined that the multi-agency counter-terrorism operations in Kenya had yielded far-reaching positive impacts for the Country in the recent past. In particular, the frequency with which the terrorists would carry out attacks, almost at will, in the Country has also notably reduced significantly. Mwangi (2017) added that without proper coordination in place, the multi-agency approach is likely to fail; adequate understanding between the various units in the multi-agency team is, therefore, of extreme importance in tracking the terrorists' activities and in identifying and apprehending the culprits involved.

Sensitization and Awareness Programs

The study further sought to establish how science and technology had enhanced community sensitization and awareness programs. The findings revealed that 24 (26.1%) of the respondents opined that science and technology had significantly contributed to Sensitization and Awareness.

The Findings were supported by officers who, in interviews, revealed that there had been community engagement and collaboration through sensitization and Awareness programs. The findings indicated that a community-focused approach involving active participation and cooperation between the government and local communities was essential for effectively addressing the issue of violent extremism. The Interview showed that the NCTC uses software tools to monitor social media and other online platforms to detect extremist propaganda and recruitment activities. The Kenyan Government has also set up a hotline number and an online reporting platform for citizens to report suspicious activities or behavior that could be linked to violent extremism. The Government has also used biometric technology through the digital forensic laboratory to identify, track suspects, seize, acquire, and analyze all electronic devices used in improvising explosive devices and prevent the extremists from crossing borders.

It also emerged from the Interviews that international organizations such as the United Nations (UN) and the United States Agency for International Development (USAID) have provided technical assistance and training to Kenyan security agencies on using technology to counter violent extremism. For instance, USAID has implemented a program that uses data-driven approaches to identify and address the root causes of extremism. Furthermore, enhancing community engagement alongside awareness and sensitization efforts is crucial. Notably, among the strategies mentioned, only a limited number specifically target the Boni forest communities. The data indicates a lack of substantial efforts in harnessing the potential of communities to counter violent extremism. The Government's current approach to countering violent extremism is primarily focused on communities. Still, it lacks a comprehensive community-centered strategy that fosters partnership and trust between the government and local communities.

The findings concur with Bilazarian (2020), who suggests that there are three ways through which technology, specifically social media, can help offer counter-narratives to radical messages. First, counter-violent extremism (CVE) initiatives gain advantages from adopting a network-oriented strategy, wherein a diverse group of individuals extensively linked within their social circles are leveraged to propagate

opposing narratives. Secondly, interactive and person-to-person communication methods assist in overcoming barriers to engagement within CVE undertakings. Lastly, messages and stories aimed at countering extremism tend to achieve greater acceptance when they align with broader community interests and priorities rather than being solely fixated on acts of terrorism or violent extremism.

Increased surveillance along and within the Boni forest

The study sought to establish whether there used increased use of technology in surveillance along and within the Boni forest. The findings in Table 4.1 revealed that 24 (26.1%) of the respondents agreed that there was increased surveillance.

It also emerged from the Interviews that surveillance technologies such as drones, CCTV cameras, and biometric systems were effective tools to monitor activities in high-risk areas and identify potential threats. Furthermore, implementing robust cyber security measures was deemed necessary to safeguard against cyber-attacks orchestrated by extremist groups. This includes securing government networks and data and educating the public on safe online practices. Promoting science and technology education in schools and universities is another national approach that helped to develop a skilled workforce to counter violent extremism. This created opportunities for young people in the region, reducing the likelihood of radicalization.

States have acquired the most advanced defense technologies in hardware and software for their security agencies by leveraging their capacities to maintain national security. Additionally, technology has revolutionized the way security is maintained. With drone technology, all-powered surveillance systems, and data analytics in security decision-making, science, and technology have enabled predictive measures that help prevent security breaches and improve the response to security breakdown. However, with technological advancements come new security challenges such as cyber-attacks, data breaches, acts of terrorism, and privacy concerns. As technology evolves, it is essential to integrate scientific advancements into security practices to protect critical systems and sensitive information.

The findings agreed with a publication from the United Nations Office of the High Commissioner of Human Rights (OHCHR) dated 14 March 2023 which stated that technology, including biometrics data sharing and drones, had provided benefits, particularly in intelligence, surveillance, and targeting. The international community could not afford to be second in a race towards a technological edge to combat terrorism.

Surveillance is also done on financial activities that could be seen as supporting terror-related activities. According to UNDOC (2021), the mobile money transfer system known as M-Pesa has significantly transformed the Country's financial banking system in Kenya. However, this technology has the potential for misuse, as it can be exploited for crowdfunding activities to swiftly and efficiently solicit and transfer funds. According to a report from Columbia Business School, the Kenyan mobile money transfer system, specifically Safaricom M-Pesa, might have played a significant role in financing the terrorist attack at Nairobi's DusitD2 hotel on 16 January 2019. Multiple news sources have indicated that court documents allegedly accused the suspects of engaging in financial fraud. In the final three months of 2018, before the DusitD2 attack, an individual acting as an M-Pesa agent registered 52 M-Pesa accounts and received Ksh. 9 million (equivalent to approximately $90,000). On a single day in January 2019, this agent utilized Diamond Trust Bank to withdraw 13 separate amounts of Ksh. 400,000 ($3,984) each, totaling Ksh. 5.2 million ($51,793). Consequently, the bank's branch manager faced charges for failing to report suspicious withdrawals as required by regulations. This incident underscores the potential misuse of the M-Pesa system for illicit activities like terrorism financing.

In as Much as MPESA could provide a loophole for crowd funding which could be a leeway for extremist groups in the Country to raise money, it also provides a technological platform through which irregular

transactions could be flagged by authorities to stop such terror activities. Partnerships between financial institutions and security agencies may come in handy to help in this. For example, through mobile money transactions, it would be easy for security agencies to track down terrorists and pinpoint their operations' locations and hence be able to make arrests and foil attacks.

Nyumba Kumi Policing

The study sought to establish how Government initiatives had embraced the use of the commonly used initiatives of Nyumba Kumi policing in Lamu County. 16 (17.4%) of the respondents stated that the Government used the Nyumba Kumi policing initiative. The respondents further opined that Science and technology tools were being utilized in various ways to counter violent extremism. One example was using social media monitoring tools to identify and track extremist groups and their activities. The county government of Lamu has also developed a mobile phone application called "Nyumba Kumi" that allows citizens to report suspicious activities in their localities (Truth, Justice & Reconciliation Commission, 2013). Additionally, the Government has invested in research to understand better the factors contributing to radicalization and develop effective prevention and intervention strategies. Furthermore, the Government has established a cybercrime unit that uses advanced technology to investigate and prosecute individuals who use the internet to promote violent extremism.

These findings were in tandem with Amit *et al.* (2021), who opined that concerning CVE through Technology, diverse collections of initiatives or schemes exist, with categorizations that can be based on varying perspectives. They added that online programs addressing Countering Violent Extremism (CVE) are typically classified into two primary groups: affirmative and restrictive measures. Affirmative measures encompass tactics that contest extremist narratives and content by creating opposing material (Hussain & Saltman, 2014). On the contrary, restrictive measures encompass strategies to hinder, sift, eliminate, or censor extremist content.

In contrast, Saltman & Russell (2014) propose a tripartite classification system for CVE programs that can be adopted by the Government, delineating them into three groups: limiting measures, which involve obstructing, censoring, filtering, or withdrawing online content; affirmative measures, encompassing counter-messaging that can be either specific or generalized; and monitoring, which entails recognizing and evaluating extremist content. This framework incorporates a "monitoring" element in addition to the classifications found under affirmative and restrictive measures. In this schema, 'monitoring' involves permitting the dissemination of extremist content while subjecting it to analysis to provide insights for counter-extremism initiatives (Saltman & Russell, 2014). Meanwhile, focusing exclusively on online CVE measures with a negative slant, Denoeux and Carter propose a categorization that segregates the most commonly utilized strategies into three segments: eradicating extremist content from the internet, managing and filtering information exchanges and user access, and concealing radical content through manipulation of search engine results.

An alternate classification framework for online CVE, formulated by Briggs and Feve (2013), presents the entire gamut of activities as a 'Counter Messaging Spectrum.' This spectrum encompasses government strategic communications aimed at propagating positive portrayals of government actions, alternative narratives that counter extremist messaging by reinforcing societal values, and counter-narratives that disassemble extremist narratives. In this schema, the Government is primarily responsible for strategic communications, while civil society is responsible for counter-narrative-related efforts.

CONCLUSION

The study concludes that science and technology are at the heart of countering violent extremism in this digital age. In as much extremist groups use modern technology advancements in furthering their agenda,

the same tech infrastructure can be used by security agencies to track and stop terrorist activities in myriad ways, as seen from the findings. In this regard, better monitoring and surveillance of technological infrastructure such as social media and other communication mediums by the government and security agencies is key to ensuring a safer society. Additionally, local and international stakeholder cooperation and collaboration have proved helpful in CVE efforts.

RECOMMENDATION

The study recommends that countering violent extremism (CVE) requires a holistic approach integrating science and technology with other strategies like community engagement, education, and policy initiatives to achieve comprehensive outcomes. Continuous research and collaboration are crucial to enhance the effectiveness of technological interventions. The government and civil society organizations should utilize various technical and scientific tools to monitor online platforms and social media for extremist content and radicalization. Employing machine learning and data analytics can help identify potential threats to national security by analyzing patterns and behaviors. Additionally, science and technology can play a vital role in preventive measures, offering education and counter-narratives through online programs and initiatives targeting vulnerable populations. However, it is essential to acknowledge that the strategies mentioned in the study do not adequately address the specific challenges faced by the Boni forest communities. There is a need for a more comprehensive community-centered approach that fosters partnership and trust between the government and local communities in countering violent extremism.

REFERENCES

1. Amit, S., Barua, L., & Kafy, A. A. (2021). Countering violent extremism using social media and preventing implementable strategies for Bangladesh. *Heliyon, 7*(5).
2. Bilazarian, T. (2020). Countering violent extremist narratives online: Lessons from offline countering violent extremism. *Policy & Internet, 12*(1), 46-65.
3. Briggs, R., & Feve, S. (2013). Review of programs to counter narratives of violent extremism.
4. Constitution of Kenya (2010). Retrieved from http://digitalcommons.law.seattleu.edu/tjrc/7.(20 November 2022).
5. Denoeux, G., & Carter, L. (2009). Guide to the Drivers of Violent Extremism and Terrorism. *Washington, DC: MSI and USAID*.
6. Global Center on Cooperative Security,
Staff, http://www.globalcenter.org/experts/staff/Archived 2014-03-06(Accessed on 20 October 2022).
7. Hawkins. D. (1995). *"Preventing Violence: Prospects for Tomorrow" Sage* Publications p.21.
8. Kakonge J.O. (2017). *"The Role of Science and Technology in Countering Violent Extremism: An African Continental Perspective"* published in the African Journal of Science, Technology, Innovation and Development.
9. Kivunzi, J., & Nzau, M. (2018). International Journal of Social and Development Concerns.
10. National Counter Terrorism Centre website http/wwww.cunterterrorism.go.ke/about us". (Accessed on 29 November 2022).
11. Owen F. and Richard F. (2015) Approaching Religion in Conflict Transformation: Concepts, Cases and Practical Implication.
12. Pelling, J. (2015). *When Doing Becomes the Message: The Case of Swedish Digital Diplomacy*. In Digital Diplomacy: Theory and Practice, Routledge.
13. Ruteere M and Aning K. (2018) *"The Use of Science and Technology in Countering Violent Extremism in Africa: Opportunities and Challenges.*
14. Saltman, E. M., & Russell, J. (2014). White Paper–The role of prevent in countering online extremism. *Quilliam publication.*
15. Sandre, A. (2015). *Digital Diplomacy: Conversations on Innovation in Foreign Policy*. Rowman & Littlefield.

16. The United Nations Global Counter-Terrorism Strategy. Plan of Action to Prevent Violent Extremism. Seventieth session, Agenda items 16 and 117. accessed (08 October 2022).
17. Théroux-Bénoni, L. nd Nadia A. (2019) 'Hard Counter-terrorism Lessons from the Sahel for West Africa's Coastal States', Available at: https://issafrica.org/iss-today/hard-counter-terrorism-lessons-from-the-sahel-for-west-africas-coastal-states[Accessed 29 September 2022].
18. Truth, Justice & Reconciliation Commission, (2013). The Final Report of the Truth, Justice & Reconciliation".
19. Twitter usage statistics. Available at http://www.internetlivestats.com/twitter-statistics/(accessed 10 October 2022).
20. UNDOC (2021). The Use of Internet, Other Cyber and Digital Platforms as well as Digital Devices to Support and Commit Acts of Terrorism in Eastern Africa. available at https://www.unodc.org/easternafrica/en/Stories/new-unodc-research-paper-focuses-on-use-of-internet-and-digital-platforms-and-devices-for-acts-of-terrorism-in-eastern-africa.html Accessed on 5 August, 2023.
21. UNOHCHR (14 March. 2023). Counter-terrorism and Security Are Frequently Used To Cover for the Adoption of High-risk and Highly Intrusive Technologies, Special Rapporteur Tells the Human Rights Council. Available at https://www.ohchr.org/en/news/2023/03/counter-terrorism- and-security -are-frequently-used-cover-adoption-high-risk-and-highly#:~:text=Technology%2C%20including%20biometrics%20data%20sharing,technologycal%20edge%20to%20combat%20 terrorism. Accessed 8 August, 2023