11. From Eastern Africa to the Lake Chad-Sahel Belt: The Current and Imminent Exploitation of Digital Technology by Terrorist Groups

Rosalind Nyawira Macharia

Abstract

Africa continues to face threats from terrorist groups. High profile attacks receive significant media attention: however, there are significantly smaller, more frequent attacks that occur on a daily or weekly basis, often outside the reach or interest of mainstream media coverage. In remote areas of the DRC and Mozambique, such attacks by groups claiming affiliation to the Islamic State Central Africa Province (ISCAP) frequently go unreported, yet they are a horrendous assault on civilian populations. In Eastern Africa, Al Shabaab has persistently attacked Mogadishu and other regions of Somalia but some of these attacks are reported only through local media or radio, often through news agencies that promote narratives controlled by the perpetrators themselves. They receive little, if any, attention outside of Somalia. Mitigating the threat of physical attacks by extremist groups is a top priority. However, while physical attacks are an output and an indicator of a groups' strengths, they represent only one component of their capabilities. A narrow focus on physical attacks overlooks two important aspects of the threat landscape, cyber warfare and information warfare, which are being executed on modern technological platforms. This article examines the pervasive and evolving exploitation of modern digital technology by the notorious terrorist groups traversing the continent, from the Eastern region to the Sahel-Chad Belt. The groups use digital technology for propaganda, recruitment, and radicalization, secure communication, coordination and operational planning, intelligence collection, surveillance, reconnaissance, offensive strikes, and for illicit financing and fund transfers. The notoriety is pegged on the territorial control and number of attacks perpetrated by these groups within the last five years.

Keywords: Terrorists, Digital technology, Eastern Africa, Sahel-Chad belt

1. Introduction

Africa is a continent endowed with many resources, the most important being its people. However, it has been plagued by poverty, bad governance and security challenges. The terrorist groups operating in Africa have taken advantage of ungoverned spaces and the vacuum left by governments' inability to provide basic public goods such as security, education and health. From the Eastern part of the continent, traversing through the Central region to the West of Africa, the Sahel and the North of Africa, terrorist groups have ravaged populations and left death and desolation in their wake. Some have shown resilience in the face of sustained operations against them, while others have been degraded and morphed to different armed groups.

In Somalia, 6,000 security events (by both Al Shabaab and Government of Somalia offensive and counter-offensive) were recorded between April 2023 and March 2025, resulting in almost 15,000 estimated fatalities.[1] In the meantime, the Sahel-Lake Chad belt has attained notoriety as the epicentre of terrorist activities in the world, thanks to the many news reports on attacks by the varied groups opeating in this region. In the first half of 2024, three Sahelian states, namely Mali, Niger and Burkina Faso registered 7,620 fatalities from terrorist attacks, setting a new record.[2]

This escalation in terrorist attacks is taking place at a time of rapid development of digital technology. Modern digital technology such as Artificial Intelligence (AI), Advanced Algorithms and Machine Learning, Encryption, Virtual Reality (VR) / Augmented Reality (AR), Quantum computing, Cloud

[1] EU Asylum Report 2025 https://euaa.europa.eu/publications/asylum-report-2025EUAA, 2025.

[2] Nsaibia, H., Oughton, E., Selod, H., & Steinbuks, J. (2024). Conflict and Cell Tower Destructions in the Central Sahel Region.

Computing and Blockchain is rapidly growing, becoming more accessible and widely applicable to multiple sections of society, a move that is both a boom and a bane for terrorists.

The exponetial growth in technology has become an aberrant motility; the increasing internet access and the high-speed connectivity, Virtual Private Networks (VPNs), the dark net amongst others are all part of the enabling infrastructure. It is now easy to anonymise and secure communication, mask locations and encrypt internet traffic, bypass geographic restrictions and surveillance efforts and create illicit networks for the trade of weapons, illegal goods, and stolen data, as well as extremist ideologies and operational strategies.

Terrorists are part of the nefarious actors that benefit from the bountiful and easy access of modern digital technology. Terrorist groups in Africa are already exploiting technology for operations, both in kinetic and information operations. The aspirations of terrorist groups and individuals to develop cyber strategies is evident, with designated terrorist groups involvement in cyber-attacks seen as far back as Al-Qaida in the late 1990s.[3] As early as 2005, the United Nations Security Council recognized the importance of States to act cooperatively to prevent terrorists from exploiting sophisticated technology, communications, and resources to incite support for criminal acts,a concern that has been raised many times since the formulation and subsequent reviews of the United Nations Global Counter-Terrorism Strategy (A/RES/60/288).[4] In 2011, Al Qaida released a widely reported video declaring an "electronic jihad" against the United States and calling upon its followers to launch cyber-attacks against critical infrastructure in the United States. As expected, Islamic State mirrored these aspirations, with various calls throughout its rise to prominence urging supporters to hack the websites of "Western" governments.

According to the Global Terrorism Index 2025, the Sahel region remained the terrorism epicentre accounting for over half of all global terrorism deaths. Islamic State affiliates registered 71%

[3] Weimann, G. "Al Qaida extensive use of the internet" (2008) *CTC Sentinel* https://ctc.westpoint.edu/al-qaidas-extensive-use-of-the-internet/

[4] https://www.un.org/counterterrorism/en/un-global-counter-terrorism-strategy

activity in Syria and the Democratic Republic of Congo. Three of the terrorist groups responsible for most deaths in 2024 operate in Africa, namely Daesh (branded itself the Islamic State (IS)) which has active affiliates in Africa namely the Islamic State in Central Africa Province (ISCAP), Islamic State in West Africa Province (ISWAP) and Islamic State in the Sahel (ISS)). The others were Jamaat Nusrat Al-Islam wal Muslimeen (JNIM) largely operating in the Sahel, and al-Shabaab operating from Somalia.[5] Previously, most deaths in Africa had been reported to be caused by Boko Haram.[6] In August 2023, the UN panel of experts on Mali declared that the ISS had doubled the amount of territory they controlled in the country, while JNIM had continued to expand operations.[7] This information is instructiuve in identifying the notorious terrorist groups in Africa for the purpose of this study, which are the Al Shabaab, JNIM, ISS, ISCAP, ISWAP and its perennial resilient rival, Boko Haram. Imperatively, among these groups, Al Shabaab has for a long time exhibited structural resilience and adaptability to morphing situations.[8]

The Global Terrorism Index[9] report also made a major observation; that terrorist groups were rapidly adapting to emerging technologies, transforming their operations through artificial intelligence and encrypted communications. Islamic State in the Khorasan was singled out for producing AI-enhanced video content and sophisticated online magazines in multiple languages, and deploying encrypted messaging platforms and cryptocurrency for fundraising, whilst using AI to create localised propaganda aimed at foreign targets. This, it was observed, posed challenges for security services as the terrorists were increasingly exploiting encrypted apps and dark web forums for radicalisation and operational planning.[10] Another important point was the reporting that in the Western countries,

---

[5] Global Counter Terrorism Index 2024 https://reliefweb.int/report/world/global-terrorism-index-2025

[6] Ibid.

[7] Letter dated 3 August 2023 from the Panel of Experts on Mali established pursuant to resolution 2374 (2017) addressed to the President of the Security Council https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2023_578.pdf

[8] Kellar, K. R. (2024). Examining the Factors that Contribute to the Survival and Resilience of the Al-Shabaab Terrorist Organization.

[9] n. 5

[10] ibid

majority of attack perpetrators had shifted from terrorist organisations' actors to individuals without formal group affiliations, who radicalised through social media, gaming platforms and encrypted messaging apps. Potential terrorists had access to extremist content, and could organise with minimal physical contact. Algorithmic radicalisation on popular social media sites could drive users toward progressively more extreme content over time.[11]

This paper examines how the terrorist groups are engaging or likely to engage with modern digital technology to their advantage. It starts with the terrorist groups in Eastern Africa and extends to the ones in the Lake Chad-Sahel belt. This approach is justified on four grounds. First, the major group in Eastern Africa, Al Shabaab is way ahead of other terrorist groups in terms of structural and operational adaptability.[12] Secondly, that terrorist organisations have been known to replicate modus operandi from other successful actors, and thus it is natural that others in Africa would copy from Al Shabaab. Third, the Eastern region of the continent connects geographically to the Lake Chad-Sahel belt, which is currently in the throes of terrorism. Finally, several countries along that belt are currently experiencing political or socio-economic fragility, notably Somalia, the Sudan, South Sudan, Chad, Niger, Mali and Burkina Faso, providing ungoverned spaces that terrorists are generically known to exploit. The study also proposes measures to counter the exploitation of digital technology by these groups.

2. Theoretical Framework

This study is grounded in Sociotechnical Systems Theory and Opportunity Structures Theory**,** which together provide a lens for examining how terrorist groups from Eastern Africa to the Lake Chad–Sahel belt might integrate emerging digital technologies into their operational ecosystems. Sociotechnical Systems Theory argues that technological tools and human actors co-evolve, shaping and reshaping

[11] Ibid.
[12] n. 7

each other's behaviour and capacities.[13] As digital platforms become more accessible, terrorist organisations strategically adapt these technologies to optimise recruitment, propaganda dissemination, operational coordination, and resource mobilisation. Opportunity Structures Theory further posits that violent non-state actors exploit enabling environmental conditions, such as weak state capacity, unregulated digital spaces, porous borders, and socio-political fragility to expand their tactical and strategic options.[14] Applied to Eastern Africa and the Lake Chad–Sahel belt, these theories illuminate how the diffusion of digital technology interacts with structural vulnerabilities (limited cybersecurity governance, uneven digital literacy, and persistent conflict) to create current and imminent avenues for technology-enabled terrorism.

3. Methodology

This study adopts a desktop research design, relying exclusively on secondary data sources to examine how terrorist groups in Africa are exploiting technology. Data were collected from a wide range of open-source materials, including peer-reviewed journal articles, think tank reports, government and intergovernmental publications, policy briefs, media articles, and databases such as Armed Conflict Location & Event Data (ACLED), CTC Sentinel, and the Global Terrorism Index.

The sources were identified through systematic searches in academic databases and complemented by grey literature from reputable organizations such as the United Nations (UN), European Union Agency for Asylum (EUAA), International Centre for Counter Terrorism (ICCT) and major international news outlets. Selection criteria prioritized recency (2020–2025), relevance to African terrorism and technology use, and credibility of the authoring institution.

---

[13] Bostrom, N., & Yudkowsky, E. (2014). *The ethics of artificial intelligence*. In K. Frankish & W. Ramsey (Eds.), *The Cambridge Handbook of Artificial Intelligence.* Cambridge University Press.

[14] Della Porta, D. (2013). *Clandestine Political Violence*. Cambridge University Press (17).

A thematic analysis approach was employed to synthesize findings across different sources. Information was organized around key themes, including terrorist use of social media, encrypted communications, drones, cyber operations, and propaganda dissemination. Triangulation was applied by cross-checking insights from multiple sources to ensure accuracy and minimize bias.

The desktop research approach was chosen for its feasibility, breadth of coverage, and ability to consolidate dispersed knowledge on the subject. However, the methodology was limited by reliance on secondary data, which may contain inherent biases, gaps in reporting, or restricted access to classified information.

4. Notorious Terrorist groups in Africa

4-1 Eastern Africa

Harakat al-Shabaab al-Mujahideen – Movement of Youthful Fighters (Al-Shabaab)

Al Shabaab is a terrorist group based in Somalia and operating in the Eastern Africa region. It came into force in 2006; its origin is intertwined with the fall of the Siad Barre regime in Somalia in 1991 and the descent into anarchy and state failure, and the balkanisation of Somalia on clan basis, each clan having its own militia. The ensuing vacuum was filled up by clan elders who sought to bring a sense of order in their areas of jurisdiction. The United States of America sent an intervention force in Somalia in December 1992 as part of Operation Restore Hope to arrest the deteorating humanitarian situation but the warlords and their militia resisted and eventually the US withdrew its troops.[15]

The collapse of the Somali government coincided with the birth of an Islamist movement following the defeat of the Soviet Union in Afghanistan by an American-funded proxy made up of youthful fighters, the Taliban Mujahideen. This victory attracted financiers, key amongst them Usama Bin Laden, the Saudi rich citizen who adopted a cause of ridding the Arab lands of foreign military.

[15] Joseph, D., & Maruf, H. (2018). *Inside Al-Shabaab: the secret history of Al-Qaeda's most powerful ally*. Indiana University Press.

Afghanistan became the base of the resistance against foreign occupation, and Usama and other Islamists started the Al Qaida organisation.[16]

Usama was eventually expelled out of Saudi Arabia and set base in Sudan in the early 1990s, and took keen interests on the tragic state of political affairs in neighbouring Somalia. The 1993 resistance of US intervention by warlords in Somalia put Somalia on the global map of armed resistance. Usama sponsored Somali youth to go and join the Afghan Mujahideen under the tutelage of Abdalla Azzam, a key Al Qaida figure credited as the father of 'global jihad.' The Somali youth came back and set up the first military training base in Kismayu town of Somalia in 1996. They eventually took over the courts that Somali clan elders had set up to adminster their areas , especially on matters of personal laws such as property disputes and marital issues. These Al Qaida ideologues also took up the militant wing of *Al Itihad Al Islamiya*, which was a movement started by senior political figures in Somalia hoping to bring order.[17]

After the 9/11 attacks, the US kept a keen eye on affairs in Somalia, concerned that Al Qaida might establish a base there. Efforts by the Al Qaida ideologues to take over Somalia were thwarted by an international alliance composed of the US and its allies, Ethiopia and warlords who drove out the ideologues from the Islamic courts and reverted them to elders. The ideologues and their recruits regrouped and in 2006, formed the Al Shabaab. The later eventually pledged allegiance to Al Qaida under the then leader. Mohamed Abdi Godane who was killed in an airstrike in 2014.[18]

Al Shabaab has been responsible for multiple attacks in and out of Somalia. Within Somalia, Al Shabaab has been responsible for many complex attacks ranging from the use of explosives to other attacks of smaller magnitude but no less severe, such as assassinations. Externally, Kenya bore the brunt of successive complex and small attacks over a period of two decades. Their first external attack,

---

[16] Tripathi, D. (2011). *Breeding ground: Afghanistan and the origins of Islamist terrorism.* Potomac Books, Inc.

[17] n.13

[18] Harper, M. (2019). Is anybody listening? Al-Shabaab's communications. In M. Keating & M. Waldman (Eds.), *War and peace in Somalia: National grievances, local conflict and Al-Shabaab.* Oxford University Press.

however, was in Kampala, Uganda, in 2010 against football fans in several restaurants during the world cup season.[19]

Their tactics include complex assaults, improvised explosive devices, assassinations, taxation/extortion, parallel justice system and sophisticated media operations. They have over the years consolidated lots of finances through taxation of commercial activities including the transportation of goods, extorting businessmen and telecommunication companies, smuggling and donations from the disapora.[20]

Despite many offensives against Al Shabaab in Somalia, the latter has remained resilient in Central and Southern Somalia; and has continued to hold ground, carry out attacks especially in Mogadishu and hold its sway against the Somali Federal Government.[21]

Allied Democratic Forces (ADF/IS-DRC)

The purpoted branch of Islamic State in the Democratic Republic of the Congo is just a morphology of a long existing insurgent group called the Allied Democratic Forces (ADF), formed in the late 1995 as a rebel group fighting against the Ugandan government of President Yoweri Museveni and led by Jamil Mukulu.[22] These fighters fled Uganda following persistent security crackdown and moved into eastern DRC. When the IS jihadist wave started in 2013, the ADF intensified its attacks against civilians and in 2017, it swore allegiance to IS Core which recognised ADF as a part of the IS in Central Africa province (ISCAP). Mukulu was arrested in 2015 but the activities of the group persisted.[23]

The ADF has undertaken many attacks in Eastern DRC, raiding homes in search of food and recruits, indiscriminately killing civilians including women and children, leaving desolate entire villages.[24]

---

[19] Ibid

[20] Badurdeen, F. A. (2023). Al-Shabaab Financing: Sources, Methods, and Countering terrorist Financing. In *Countering Terrorist and Criminal Financing* (pp. 483-496). CRC Press.

[21] Ibid.

[22] Weeraratne, S., & Recker, S. (2018). The isolated islamists: The case of the allied democratic forces in the ugandan-congolese borderland. *Terrorism and Political Violence*, *30*(1), 22-46.

[23] Ibid.

[24] Bolmvall, N. (2025). Explaining Violence: A qualitative case-study of the ADF's rebel violence against civilians.

Most recently, in late July 2025, ADF fighters killed dozens of people, including women and children, during a night-time church gathering in Komanda, Ituri province. The attack also involved abductions and the burning of homes. This incident, and others like it, highlight the group's brutal tactics and a shift toward targeting Christian communities.

[25]ADF has exploited the confusion and vested interests of the various armed groups fighting in the DRC, including the Congolese army (FARDC) and the M23 armed group. International attention has been hoarded by these later groups, leaving ADF to move undettered. Any attempt to push back ADF is met with mass-casualty attacks on civilians.[26]

The ADF has expanded its area of operations from its traditional strongholds in North Kivu into the remote forested areas of Ituri province, and this inaccessibility has increased their propensity for violent atacks. Its tactics include massacres, abductions and attacks along roads and in villages. In the last three years, it has used improvised explosive devices to attack targeted civilians in Uganda and the DRC, and has worryingly shown a growth in expertise in the assembly of IEDs, an indication that it might have received ied trainers from other extremist theatres. It is projected that without specific measures to address this group, they will persist in their indiscriminate violence for survival and will seek to further expand to remote areas to ensure operational freedom.[27]

ISIS-Mozambique (Ahlu Sunna wa-Jama'a)

ASWJ, (adherents of the prophetic tradition) is a group of Mozambican youth that emerged in 2017 in the Northern Province of Cabo Delgado, Mozambique. The youth were largely poor, unemployed and claimed political marginalisation. It was heavily influenced by the teachings of Islamist leaders in the coastal areas of the neigbouring countries, and a wave of defections of the East African swahili speaking foreign fighters from Al Shabaab in Somalia. This followed a crackdown by Al Shabaab on foreign fighters

[25] Winter J. & Makumeno E., (2025) More than 40 killed in DR Congo attack linked to Islamic State https://www.bbc.com/news/articles/c3ezjg34lw4o

[26] (UN report on DR Congo situation, (2025) https://news.un.org/en/story/2025/07/1165511.

[27] n. 22.

who were accused of spying for international partners and thus causing an increase in aerial attacks on Al Shabaab.[28]

With the support of some of those who escaped from Al Shabaab and the security dragnet in neighbouring countries, radicalisation, and recruitment efforts started in earnest, followed by attacks on villages in the areas of Cabo Delgado and Mocimboa de Praia provinces.[29] At the height of their operations, they raided hotels and oil infrastracture. In 2019, IS core formally recognized them as its Central Africa Province (ISCAP), a designation shared with the ADF.[30]

Their tactics include attack on civilians, ravaging entire villages with massacres, beheadings, and abductions, leading to massive population displacement. They have also targeted strategic assets, for instance in March 2021, the group captured the port town of Palma, a hub for a multi-billion dollar natural gas project, thrusting them into international limelight and causing Southern African Development Community (SADC) countries to consider a multinational force to stop the spread of terror. A regional force under SADC was launched, and troops from Rwanda and South Africa were deployed to support the Mozambican government efforts. These efforts have largely borne fruits, with a reduction in violent incidents save for small pockets that are resilient.[31]

On 10 May 2025, IS core claimed that its Mozambique affiliate had killed 11 Mozambican soldiers during an attack on a Forças Armadas de Defesa de Moçambique/Mozambique Defence Armed Forces (FADM) position outside the village of Miangalewa, located in Cabo Delgado province. Local media confirmed this attack but indicated that the death toll may be as high as 18.[32]

---

[28] Guhad, H. A. (2025). Terrorism in Mozambique: Evolution, context, and prognosis. In *Palgrave Handbook of Terrorism in Africa* (pp. 519–538). Springer Nature Switzerland.

[29] Bukarti, B., & Munasinghe, S. (2020). The Mozambique conflict and deteriorating security situation. *Tony Blair Institute for Global Change*, *19*.

[30] Ibid.

[31] Svicevic, M. (2024). The SADC mission in Mozambique. *Mozambique's Cabo Delgado Conflict: International Humanitarian Law and Regional Security*.

[32] ACLED, Cabo-Ligado update 5-18 May (2025) https://acleddata.com/update/cabo-ligado-update-5-18-may-2025

4-2 Lake Chad Basin

Jama'atu Ahlis Sunna Lidda'awati wal-Jihad (Boko Haram)

Boko Haram was founded in 2002 by a Nigerian cleric called Mohammed Yusuf in Maiduguri, Borno State, Nigeria. It began as a religious sect, *Jama'atu Ahlis Sunna Lidda'awati wal-Jihad* ("People Committed to the Prophet's Teachings and Jihad"). It was extremely against the western culture which it blamed for the high corruption in Nigeria. It forbid western education, thus acquiring a nickname from the locals, *Boko Haram*, meaning "Western education is forbidden". It attracted many poor and unemployed youth and actively radicalised them. It started a campaign of violence, and in 2009, a clash between them and security forces led to the death of Yusuf and hundreds of his followers. Abubakar Shekau took over as the new leader.[33]

At the height of its operations, Boko Haram carried out an atrocious insurgency in northeastern Nigeria, through raids and explosive attacks on civilians (including churches and schools) and security forces. In 2011, it attacked the UN headquarters in Abuja using a vehicle-borne improvised explosive device (VBIED), causing concern that it has extended its campaign to the urban areas.[34]

It kidnapped civilians; one of the infamous incidents was the April 2014 attack on a school called Chibok girls school and kidnapping of hundreds of school girls who became brides for the fighters. This sparked a global rallying call to bring the girls back home under the banner "Bring Back Our Girls." The same year, it occupied the region of Damasak and killed over 400 civilians during the months of occupation. Boko Haram has killed tens of thousands of people, and displaced over 2 million people in Borno, Adamawa, and Yobe.[35]

---

[33] Sergie, M. A., & Johnson, T. (2015). Boko Haram. *Council on Foreign Relations.*

[34] Iyekekpolo, W. O. (2016). Boko Haram: Understanding the context. *Third World Quarterly, 37*(12), 2211–2228.

[35] Ajiboye, B. M. (2022). Boko Haram: Shekau's Demise–Halcyon or Nadir for Sub-Saharan Africa's Fight Against Terrorism?'. *Conflict Studies Quarterly*, *41*, 3-14.

In 2015, Boko Haram pledged allegiance to Islamic State and its then leader Abu Bakr Al Baghdad and renamed the group as the Islamic State West Africa Province (ISWAP). However, Shekau's extreme tactics, i.e. using women and children as suicide bombers and mass killings, clashed with IS core's strategy and in 2016, the latter recognised Abu Musab al-Barnawi (son of Boko Haram founder Mohamed Yusuf) as the new ISWAP leader. Consequently, Shekau broke away and revived Boko Haram under his control. He was killed in 2021 following a clash between the factions. Boko Haram rebounded under commander Bakura Doro, and reclaimed control over many islands in the Lake Chad area.

Boko Haram has been on a steady decrease and is left with pockets of fighters, a fading shadow of its former self. However, these fighters still engage in acts of violence. Suspected Boko Haram insurgents remain active in their stronghold regions of Yobe and Borno states.[36]

Islamic State in West Africa Province (ISWAP)

As ISWAP got financial and propaganda support of IS core, it increased its recruitment drive, targeting young people, especially poor teenage boys and girls. Unlike Boko Haram, ISWAP avoided civilian casualties and focused on military targets, propaganda, and gaining popular support. It took control over multiple military bases in northeastern Nigeria (2018–2019), and established shadow governance, including taxation and provision of limited services, in Lake Chad regions spanning Nigeria, Niger, Chad, and Cameroon.[37]

In March 2019, internal wrangles led to the replacement of Abu Musab al-Barnawi with Abu Abdullah ibn Umar al-Barnawi. The removal of Abu Musab triggered an exodus of ISWAP's top fighters, led by Adam Bitri, a skilful military commander. He unsuccessfully sought collaboration with ANSARU, an earlier militant group that worked closely with Al Qaida and set up a base in Abadam, Borno state,

[36] Ibid.

[37] Kelly, F. (2019, March 15). Islamic State enforced leadership change in West Africa Province, audio reveals. *The Defense Post.* https://www.thedefensepost.com/2019/03/15

Nigeria to confront ISWAP. In March 2019, ISWAP merged with the Islamic State in the Greater Sahara (ISGS) to form the "Greater Sahara Faction" but later parted ways.[38]

In May 2025, ISWAP launched assault against military installations, towns and roadways seizing control of strategic sites in Borno, abducting soldiers and reinforcing their foothold near Lake Chad's critical smuggling routes. As of June 2025, ISWAP was dominant in the Lake Chad region, using sophisticated technology and raising finances through extortion rackets and taxations of businesses along transport corridors.[39]

4-3 The Sahel

Jama'at Nusrat al-Islam wal-Muslimin (JNIM)

JNIM was formed in 2017 out of a merger of Islamist factions in the Sahel region, consisting of Ansar Dine, Al Murabitoun, Katiba Macina (Macina Liberation Front) and Al-Qaeda in the Islamic Maghreb (AQIM)-Saharan wing. The founder and leader of Ansar Dine, Iyad Ag Ghaly was appointed the leader (amir). The merger was a strategic survival tactic followed sustained military pressure from the French troops which disrupted jihadist bases in Northern Mali. The coalition is a cocktail of ethnicities, including the Tuaregs, Fulanis and Algerians spanning across the region.[40]

JNIM pledged allegiance to Al Qaida and it's the leader Ayman Al Zawahri; the merger was approved by Al Qaida in 2017. They operates in the vast areas of Mali, Burkina Faso, Niger and spills over to Benin, Togo and Côte d'Ivoire. They employ a variety of tactics, including sieges/raids, IEDs,

---

[38] Barkindo, A. (2023). Boko Haram-ISWAP and the Growing Footprint of Islamic State (IS) in Africa. *Counter Terrorist Trends and Analyses*, *15*(2), 12-17.

[39] Ukaeje, O. (2025). State and the terrorist threats in Chad. In *Palgrave Handbook of Terrorism in Africa* (pp. 83–107). Springer Nature Switzerland.

[40] Tripodi, S. (2025). Explaining the resilience of insurgent organisations using a four-function paradigm: The case of Jama'at Nusrat Al-Islam wal Muslimin (JNIM).

roadblocks, targeted assassinations, negotiated co-existence and parallel administration. They finance their operations through taxation, cattle/commodity levies, smuggling and ransom.[41]

JNIM has alarmingly expanded its operations in the period between January to June 2025. It has overrun major cities in Burkina Faso and Mali. In April 2025, it carried out the deadliest-ever attack on soldiers in Benin at the border with Burkina Faso and Niger. On 11 May, It overran a military base in Djibo town, Burkina Faso killing up to 200 soldiers, and assaulted eight other locations, killing 60 soldiers. On 1 June 2025, JNIM attacked Mali's military base in Boulkessi, near the border with Burkina Faso, killing approximately 60 security personnel, and the following day, it struck multiple military sites in Timbuktu. On 1 July 2025, it coordinated attacks targeting installations in Mali's Kayes and Ségou regions.[42]

Burkina Faso has been the country most affected by JNIM violence, both in 2024 and 2025. The government response of using tribal militias to suppress them has been counter productive since the militias target the Fulani Muslim minority, and as a result the Fulani have joined JNIM for protection. Niger amd Togo have also reported a marked increase of terrorist activities. JNIM is threatening even some of the peaceful West African neighbouring states such as Ghana, Cote d'Ivoire, Guinea and Senegal.[43]

According to Nsaibia et al,[44] JNIM are creating a quasi-state that stretches like a belt from Western Mali all the way to the borderlands of Benin. They have expanded their territorial influence; carried out periodic seizures of towns and used an adaptive "embedded" strategy within the broader West African concept. They have established a presence in Burkina Faso, Mali, Ivory Coast, Benin and Togo and are expanding to Guinea, Senegal, Ghana and Mauritania. JNIM have the operational capability

[41] Afriyie, F. A. (2023). A tale of two jihads: Unraveling the atrocities of Islamic State in the Greater Sahara (ISGS) and Jama'at Nasr al-Islam wal Muslimin (JNIM) in the Sahel. *Austral: Brazilian Journal of Strategy & International Relations, 12*(23).

[42] UN Security Council report, July 2025 https://www.securitycouncilreport.org/atf/

[43] Ibid.

[44] n. 2

to conduct complex attacks with drones, improvised explosive devices and large numbers of fighters against well-defended barracks. They have increasingly relied on an encirclement strategy to expand influence across the Sahel, particularly in Mali, Burkina Faso, and Niger. This strategy involves gradually isolating state forces and local communities by cutting supply routes, coercing civilian cooperation, and establishing parallel governance structures in contested rural spaces. Rather than seeking rapid territorial conquest, JNIM uses incremental territorial asphyxiation, targeting military outposts, ambushing convoys, and controlling key roads to render state presence unsustainable and force security forces into retreat.[45]

Islamic State Sahel Province (ISSP; ex-ISGS)

The expansive Sahel region is a complex one, with security challenges juxtaposed with difficult climatic conditions and high levels of poverty. It is no wonder that the Islamic State Sahel Province has found a base, in addition to other terrorist groups and militias ravaging the region.

The withdrawal of the French troops between 2022-2025 has exercerbated the situation, with IS exploiting the vacuum left in the tri-border of Liptako-Gourma, particularly in the northern parts of Mali's Menaka region. IS Sahel started as the Islamic State in the Greater Sahel (ISGS) (2015-2019), then merged with Islamic State West Africa Province (2019-2022), but later established itself as the autonomous Sahel Province of the Islamic State with a focus on consolidating territorial control (2022-present).[46]

Though the group has faced airstrikes that have led to the death of key leaders, it has sought to consolidate territory and incorporate all ethnicities in their leadership structures including the Fulani, Arab, Tuareg, Dawsahak, Songhai, and Djerma ethnic groups.[47]

---

[45] Thurston, A. (2020). *Jihadists of North Africa and the Sahel: Local Politics and Rebel Groups*. Cambridge University Press.

[46] Meyer, A., Simonet, L., & Späth, J. (2025). The European Union and the Sahel: The day after. www.ssoar.info

[47] Bere, M. (2024). The Islamic State in the Sahel. *Perspectives on Terrorism*, *18*(2), 137-150.

It operates in remote areas and as such does not pose existential security challenges to the capitals of Mali and Burkina Faso, but poses a threat to Niamey, where it has conducted sporadic operations, including raids and suicide bombings in 2016 and 2019, and a prison break at the Koutoukale high-security prison in 2024, about 40 kilometers northwest of Niger's capital. It raises finances through looting, taxation and smuggling.[48]

Government forces, supported by the former Wagner mercenaries (now Africa Corps) and pro-government militias, have carried out air and ground assault against IS Sahel, leading to significant losses. There has also been a serious clashes with JNIM over territorial control, with both sides regsitering casualties.[49]

5. Exploitation of Modern Digital Technology by the aforementioned Terrorists Groups

Digital technology in the contemporary world is evolving and developing rapidly, becoming more accessible because it is cheaper and easier to use. It has the potential to be disruptive and change norms at a pace that outruns laws and policies.

Terrorists are exploiting this technology in various ways. Disinformation campaigns, automated propaganda, enhanced recruitment, surveillance and targeting, translation, development and distribution of training manuals, developing and launching malware and using software on demand are just some of the ways terrorists are interacting with modern technology.[50] Extremist groups frequently utilize social media, fake news, and manipulated content to spread their ideology, recruit members, and sow discord among communities. During or in the aftermath of attacks, extremist groups often control narratives through masterful use of social media platforms and content posted on other digital spaces.

---

[48] Ezra, M. (2025). Central Sahel: An equation of crises for a sum of paradoxes. *The African Geopolitical Atlas 2025: Conflicting Information, Conflicted Realities.*

[49] Ibid.

[50] Liang, C. S. (2022). Technology and terror: The new arsenal of anarchy. In *Handbook of Security Science* (pp. 1–24). Springer, Cham.

These platforms enhance their communication infrastructure, allowing them to amplify their messages and propaganda by exploiting algorithms in ways that shape public opinion and maintain influence. The ability to quickly disseminate information and influence public perception can be more effective in promoting their agenda than the attacks themselves.[51] Hence the internet has brought a new face into the process of radicalisation and recruitment, as it creates networks and acts as a 'virtual glue' to the members of a group.[52]

Al-Shabab is considered one of the most sophisticated actors in the way they use the internet and share their content. According to a Tech Against Terrorism report in 2024,[53] in any given week, around 20 to 25% of the content that Tech Against Terrorism found on the internet had likely been generated by al-Shabab, making it essentially the largest single producer of terrorist material on the internet.

Some of the key digital technologies that terrorists in Africa have or are likely to interact with include Artificial Intelligence (AI), Advanced Algorithms and Machine Learning , Encryption, Virtual Reality (VR) / Augmented Reality (AR), Cloud Computing, Blockchain, Surveillance technologies (biometrics, drones, satellites) and Cyber tools (hacking, digital forensics).

5-1 Surveillance tools (Iot, Drones, Satellites)

The cyberspace has become an important domain of warfare, with cutting edge technology being developed and tried in major conflict zones. The Russia- Ukraine conflict has become a warfare technology-testing ground, including use of "smart drones" using Artificial Intelligence assistance.[54] Autonomous drones are more precise, and more accessible than they were previously. Drones have

[51] Ibid.
[52] Sageman, M. (2004). Understanding Terror Networks. Philadelphia: University of Pennsylvania Press
[53] Tech Against Terrorism Analysis (2024) https://techagainstterrorism.org/analysis

[54] Ulrike F. Drones in Ukraine: Four lessons for the West https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/

become increasingly integral to the operational strategies of extremist groups. Al Shabaab has embraced drone technology especially in surveillance and photography, as exhibited during the 2020 attack against an airstrip in Manda bay, Lamu county of Kenya. During this attack, Al Shabaab took and shared online drone images of the attack.[55] There have also been many reports indicating that Al Shabaab have acquired drones from the Yemen theatre for surveillance and attacks.[56] In February 2025, a UN report indicated that in Galgaduud, Somalia Al-Shabaab's reconnaissance drones were intercepted.[57] Sightings of mini and micro unarmed aerial surveillance (UAS) drones alleged to be used by the group have been reported severally. However, there is yet any evidence that Al Shabaab has used them for attacks, perhaps because their explosives tactics are working well for them.[58]

The JNIM drone use has quickly evolved from isolated surveillance to structured operations involving intelligence-surveillance-reconnaissance (ISR), direct strikes, and coordinated assaults. In September 2023, the group registered its first documented activity in Bandiagara, Mali and has since intensified the use, conducting repeated drone-enabled attacks across Mali, Burkina Faso, and Togo in 2025. These are often coordinated with ground assaults.[59]

ISWAP was reported to be using drones as early as 2019. In March 2025, they conducted a grenade-armed quadcopter in Wajikoro and Wulgo in Borno State, Nigeria, killing 12 soldiers. ISWAP has been employing UASs to conduct ISR and to record propaganda materials. In a notable incident in 2018,

---

[55] Aguilera, A. (2023, July 5). Drone use by violent extremist organisations in Africa: The case of Al-Shabaab. *GNET Insights.* https://gnet-research.org/2023/07/05/drone-use-by-violent-extremist-organisations-in-africa-a-case-study-of-al-shabaab/

[56] Allen, K. (2025). Unmanned aerial systems and violent non-state actors in Africa: Proliferation, adaptation and use. In *Drones in the African battlespaces* (pp. 125–145). Springer Nature Switzerland.

[57] Barbara MF., The Use of Uncrewed Aerial Systems by Non-State Armed Groups Exploring Trends in Africa https://unidir.org/wp-

[58] Ibid.

[59] Institute for Security Studies, "Lake Chad Basin: Insurgents Raise the Stakes with Weaponised Drones," issafrica.org, accessed June 05, 2025, https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones.

Boko Haram utilized drones for surveillance and coordination during an attack on a military base in Nigeria's Borno State.[60]

IS-Sahel deployed a drone in Tillabéri, Niger (May 2025), while ISCAP and Boko Haram rely on drones for surveillance or propaganda purposes.[61] In Mozambique's Cabo Delgado province, ASWJ was reported to deploy UAS suevrillance drones which were intercepted by the Mozambican Defence Armed Forces (Forças Armadas de Defesa de Moçambique, FADM) in 2022. The same year, the Mozambican police shot down two UASs reportedly deployed by the group that were flying over the barracks of the police's special reserve forces near Nampula International Airport .[62] The ADF in the DRC have been reported to use UASs for surveillance on different occasions since early 2021, especially to record videos and take pictures of its activities for propaganda, some of which are sent to IS core for inclusion in their infographics of caliphate wins.[63]

5-2 Artificial Intelligence

Artificial intelligence (AI) is a broad field of computer science focused on creating systems that can perform tasks that would typically require human intelligence.[64] User-facing generative AI models have made Large Language Models (LLMs) accessible and have enhanced capabilities of users to generate

---

[60] Security Council, S/2019/50, para. 103; Security Council, S/2020/50, para. 41; Soufan Center, "Intel-Brief: The Islamic State in West Africa Province is Growing in Strength and Sophistication", 2019, https://thesoufancenter.org/intelbrief-the-islamic- state-in-west-africa-province-is-growing-in-strength-and-sophistication/.

[61] Military Africa, "Africa's Insurgents and Terrorists Are Adopting Drones," militaryafrica.com, February 23, 2025 (https://www.military. africa/2025/02/the-rise-of-drone-warfare-insurgents-and-terrorists-in-africa/)

[62] Dass (May 2023); K. Allen, "Drones and Violent Non-State Actors in Africa", ACSS, 2021, https://africacenter.org/spotlight/ drones-and-violent-nonstate-actors-in-africa/.

[63] United Nations Panel of Experts on the DRC Security Council, S/2021/560, Annex 14, https://documents.un.org/doc/undoc/gen/n24/373/37/pdf/n2437337.pdf

[64] Abass, H. (2025). Artificial Intelligence in Cybersecurity: Advancements and Challenges in Data Protection. *Bilad Alrafidain Journal for Engineering Science and Technology*, *4*(2), 13-27.

content. The creation of realistic but fake videos and images for disinformation and propaganda, known as deep fakes is on the rise. Indeed, tech companies such as OpenAI are refining these applications with the aim of having them surpass human intelligence, and have combined image, audio-visual and text generation models. On 6th August 2025, Open AI Chief Executive Officer launched the latest version of their generative AI, GPT 5 and described it as the most powerful chatbot ever developed, supposed to be PhD-level smart.[65]

These LLMs can be used for spreading extremist narratives, creating fake news, or automating phishing attacks. AI-generated synthetic voices that can mimic real individuals can be used for deception and social engineering attacks.[66] Automated creation of articles, social media posts, and other content to flood information channels with extremist propaganda is now a real possibility while advanced algorithms for facial recognition to identify or verify a person's identity by analysing and comparing patterns based on their facial features are just some of the AI uses that are going to be exploited for nefarious purposes. In April 2023, the EUROPOL Innovation Lab reported some of the ways in which LLMs such as ChatGPT can be used to commit or facilitate crime, including impersonation, social engineering attacks, and the production of malicious code that can be used in cybercrime.[67]

Addressing a ministerial debate of the Security Council in 2019 on countering the threat of terrorism, United Nations Secretary-General António Guterres remarked on the "dark side of the digital world" and the "new frontier" of crime-as-a-service. He highlighted trends and developments in social media and the dark web to coordinate attacks, spread propaganda and recruit new followers.[68]

AI can be used for creation of convincing fake content that can lead to large-scale disinformation campaigns, undermining trust in media and institutions. At the same time, generative AI

---

[65] Open AI, Introducing GPT 5 (2025) *https://openai.com* › index › introducing-gpt-5

[66] Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 324.

[67] EUROPOL, How AI can strengthen law enforcement: Insights from Europol's new report (2024) https://www.europol.europa.eu/media-press/newsroom/news/

[68] United Nations, Beneath the surface: Terrorist and violent extremists use of the dark web abd cyber crime as a crime-for-service www.UNICRI.org

can create large volumes of extremist content, making it easier to flood social media and other platforms with propaganda. In June 2023, Tech Against Terrorism analysts identified an al-Qaeda (AQ)-aligned media entity that was using generative AI for propaganda production. The posts were made on a social media platform popular with violent Islamist outlets and had AI-generated images of major Al Qaida figures such as Ayman Al Zawahri (former deputy to Usama Bin Laden) overlaid on violent Islamist imagery.[69]

Al Shabaab is adept at such content creation, as shown by the many videos produced by their media wing, the Al Kataib foundation. Al Kataib produces videos during all attacks and edits them professionally and distributes them as part of their propaganda and disinformation campaigns using social media.[70]

Indeed, social media has been of great benefit to terrorists. Al Shabaab and IS had numerous posts on facebook containing propaganda.[71] Al-Shabaab also used anonymous platforms such as JustPaste.it to spread their propaganda videos.[72] Social media is also used for recruitment through circulation of videos encouraging youth to arise and fight non-believers, and to to broadcast messages asserting their power and aiming to intimidate law enforcement authorities. For instance, Boko Haram messaging targets members of the Nigerian armed forces to convince them that they are figghing a losing battle.[73] Social media is also used to solicit funds from possible fianciers and sympathisers, as Al Shabaab aptly does, ending some of its propaganda videos with requests fro funding. These groups also use social media to claim responsibility and glorify themselves as Al Shabaab does with every attack, and Boko Hamarm too.[74] In October 2021, a Somali-language 'media outlet' shared videos carrying al-

[69] Analysis reports 2023 https://techagainstterrorism.org

[70] Demirtaş, T., & Warsame, A. A. (2025). Al-Shabab's evolving media strategy: Narratives, tools, and impact (2006–2025). *SETA.*

[71] Mwale, B. (2025). The regulation of terrorist online content in Africa: an overview of the applicable regional instruments and the legal frameworks of South Africa, Kenya and Nigeria. *Journal of Policing, Intelligence and Counter Terrorism*, 1-18.

[72] Ibid.

[73] Ibid.

[74] Ayad, M. (2025). Teenage Terrorists and the Digital Ecosystem of the Islamic State. *CTC Sentinel*, *18*(2),

Shabaab glorifying their attacks, which remained on the platform for several months, attracting 53,300 views and 17,800 shares.[75] Allowing such content to remain online for long periods enables wider spread of the material.

AI-driven analysis and content generation can target and recruit individuals more effectively by tailoring messages to specific psychological profiles, thus enhancing recruitment. As far as surveillance and targeting are concerned, advanced computer vision and natural language processing can improve the ability to monitor, identify, and target individuals or groups of interest to terrorists. The translation capability within AI can be used to quickly translate text and narratives into multiple languages for distribution. Software on demand is useful for developing independent chat apps, online forums, document sharing apps, or other platforms.[76]

Al Shabaab has been translating content from Somalia language to English, Kiswahili and Arabic, especially targeting its diaspora audience.[77] In 2023, a pro-Islamic State (IS) user of an archiving service claimed to have transcribed an Arabic-language IS propaganda message using an AI-based automatic speech recognition (ASR) system and posted the material on an archiving platform that was popular with IS users to host and share propaganda. Investigations established that the transcription was initially done from Arabic speech to Arabic script.[78]

In its annual and transparency report of 2024, the Global Internet Forum to Counter Terrorism (GIFCT) wrote about the threats posed by extremist/terrorist use of Generative AI, including for propaganda purposes, where AI can be used to generate and distribute propaganda faster and more efficiently making it accessible for recruitment.[79] Tufekci[80] describes YouTube as a perfect tool for

---

1-8.

[75] Ibid

[76] Johns, A., Matamoros-Fernández, A., & Baulch, E. (2023). *WhatsApp: From a one-to-one messaging app to a global communication platform*. John Wiley & Sons.

[77] Matusitz, J., & Wesley, D. (2024). Case Study: Al-Shabaab's Digital Media. In *Jihad in Sub-Saharan Africa: The Role of Digital Media* (pp. 151-178). Cham: Springer Nature Switzerland.

[78] Tech against terrorism, (2023) Early Terrorist Adoption of Generative AI https://techagainstterrorism.org/

[79] GIFCT Our Impact in 2024 2025 https://gifct.org/2025/07/23/our-impact-in-2024/

[80] Tufekci, Z. (2018). How social media took us from Tahrir Square to Donald Trump. *MIT Technology*

radicalisation in the broad sense as it offers users more and more radical and extreme content in order to gain the maximum amount of their attention.

It is also easier to develop training manuals for nefarious purposes such as bomb-making instructions, 3D printing of firearms as well as generate and unleash malware and viruses denying services.[81] Importantly, AI can also generate pictures and videos in seconds to evade reverse image search identification successfully. AI-generated profile pictures pose a unique enforcement challenge because of detection complexity. The number of deepfakes are on the rise; the more sophisticated this technology becomes, the more difficult it is for humans to accurately differentiate between human and synthetically generated content. This offers a perfect opportunity for disinformation and misinformation to thrive. For terrorist whose extremist content may not have legitimate ways of debunking, such deep fakes achieve a level of believability and can lead to large-scale disinformation campaigns, undermining trust in media and public institutions. For instance, deepfakes of the 2002 Bali (Indonesia) bombers have emerged, re-animating the attackers to appear to be telling audiences to carry out attacks.[82]

5-3 Machine Learning and Advanced Algorithms

Machine learning (ML) is an application of AI that allows machines to autonomously learn from structured or semi-structured data and uses algorithms to produce predictive models. It is about creating algorithms that can analyze data, identify patterns, and make predictions or decisions based on that learning.[83]

Review, 14(18).

[81] n. 75

[82] McSwiney, J. (2025). Democratic Resilience in Retreat: Australia's Response to the 2002 Bali Bombings. *Political Studies Review*, 14789299251360661.

[83] n.51

Terrorists create algorithms for five purposes. First, for content personalization, tailoring propaganda messages to audiences based on their preferences and behaviors and ensuring that propaganda messages resonate more deeply with specific audiences thus increasing the impact. The algorithmic system of social media ensures that users are in social bubbles and echo chambers that keep them believing in their content to the exclusion of alternative voices. Translation apps allow for quick conversion of text and narratives into multiple languages for distribution. In December 2023, IS in their dark web publication "Voice of Khurusan" while called for global attacks against the Jews. The message in this video was well-curated to help its affiliates including those in Africa identify with the Palestinian cause.[84] Indeed, certain hacking groups such as "The Islamic State Hacking Division," the "Caliphate Cyber Army," and the "United Cyber Caliphate" have been associated wth Islamic state and have been assessed to play a key role in the group's cyber activities and played a key role in its extensive use of social media.[85]

Another reason why terrorist create algorithms is for automated moderation evasion, whereby terrorists develop techniques to avoid detection and circumvent removal of content by social media moderation algorithms. Terrorists circumvent moderation by posting in their native languages to circumvent moderation tools. This way, they hide in plain sight in online spaces, allowing the extremist content to remain online longer, increasing reach and influence. Boko Haram and Al Shabaaab have perfected this art.[86] In October 2023, the Somali government, working with tech companies started a campaign to bring down all X and facebook accounts used by Al Shabaab. Following these efforts Al Shabaab created new social media accounts and tweaked the domain names to get back online. A day after the ban, key Al-Shabaab communicants known as opinion setters advised their amplifiers to access Telegram through virtual pivate networks and flooded Telegram with new accounts and content. They

[84] Parale, Yogesh. "Analyzing the Rhetoric Posed by the ISKP in Afghanistan: A Case Study of the Voice of Khorasan." *Indian Journal of Asian Affairs* 36, no. 1/2 (2023): 41–54. https://www.jstor.org/stable/27307174.
[85] Ibid.
[86] Eichhorn, H. L. (2022). *Islamist Terrorist Organizations in Africa: A Comparative Study of Al-Shabaab and Boko Haram* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

alternatively operated the networks as public and private and frequently changed the handle names. They also resorted to using long multimedia content (video, audio) in Somali,knowing too well that content moderation tools often struggled with the Somali language content due to limited training data. They also shifted to other platforms such as the Russian social network site Odnoklassniki, abbreviated as OK.ru, but the opinion setters still controlled the narrative.[87]

Another reason why terrorists create algorithms is for sentiment analysis while analysing social media posts and communications to gauge public sentiment and adjust propaganda strategies accordingly. This helps extremist groups understand and manipulate public opinion, making their propaganda efforts more effective. Yet another reason is to enhance targeted recruitment. Behavioral analysis can identify individuals who are more susceptible to extremist ideologies, allowing for more effective recruitment strategies. AI-driven analysis and content generation can target and recruit individuals more effectively by tailoring messages to specific psychological profiles. Finally, manipulating social media algorithms to ensure extremist content is more widely seen and disseminated is also a tactic that terrorists have been known to use. For instance, more refined GenAI images are now seen across official ISIS-affiliated publications.[88]

5-4 Encryption

This involves securing communication while in transmission and ensuring secure file transfer and storage. This allows terrorists to securely plan and coordinate operations without interception, and to transfer sensitive files containing training materials, know-how, propaganda, videos, or plans. Boko Haram and ISWAP have used encrypted apps for secure communication and drones for tactical advantage.[89] Among cybercriminals, popular encryption communication platforms include Telegram,

[87] n.55

[88] Borgonovo, E., Plischke, E., & Rabitti, G. (2024). The many Shapley values for explainable artificial intelligence: A sensitivity analysis perspective. *European Journal of Operational Research*, *318*(3), 911-926.

[89] Ojo, J. S. (2024). *Convergence of Terror: Boko Haram Insurgency, Fulani Militancy, Armed Banditry, and Separatist Movement in Nigeria* (Doctoral dissertation, Doctoral dissertation, University of Portsmouth).

Signal, and Discord, with Telegram identified as a top medium of illicit cyber activity in 2023. In 2019 instant messaging service Telegram Messenger (Telegram) cracked down on several jihadist channels. In response, al-Qaeda engineered a new Rocket.Chat server, a decentralised social media platform where developers could not act on content stored on 'user-operated servers' or spread across 'the user community' and advised its affiliates on its use. This create even more secure and private communication channels and caused a major challenge to content moderation software producers.[90]

5-5 Cloud Computing

On-demand hosting and on-demand access to powerful cloud services allows self-hosting of websites and platforms developed and hosted independently of mainstream technology. Tasks and attacks can be automated using cloud-hosted bots or other on-demand cloud services. Big data analysis tools obtained from cloud resources are used for analyzing large datasets. Indeed, terrorists are operating open websites for recruitment and disseminating information as a way of circumventing social media regulations since websites are easy to register, set-up and keep online and can quickly re-appear elsewhere following disruption. Terrorist-Operated Websites are publicly available and are often indexed by search engines. JNIM is reported to use 'beacon' websites to drive Internet traffic to smaller sites and 'aggregators' to provide users with a collection of links that go to the same terrorist content.[91]

5-6 Block Chain

Cryptocurrency has been used for fundraising and disguising funds transfer for money laundering purposes. ISIS affiliates have used cryptocurrencies to circumvent traditional financial systems for financing their networks. Bitcoin was the first cryptocurrency seen to be used by these groups for crowdfunding campaigns and it remains commonplace for broader terrorist financing and money

[90] Ibid.

[91] Allen, K. (2025). Unmanned aerial systems and violent non-state actors in Africa: Proliferation, adaptation and use. In *Drones in the African battlespaces* (pp. 125–145). Springer Nature Switzerland.

laundering.[92] They have been exploring other less-traceable platforms such as the more privacy-centric Monero, which is primarily used for donation campaigns, decentralized finance (DeFi), mixing services and cross-bridging to alternative blockchains, with the widespread use of TRON and Tether stablecoin (USDT) being as a prominent trend reported by experts.[93]

In 2018, a British-South African couple, Rachel and Rodney Saunders were kidnapped and killed in KwaZulu-Natal by terrorists affiliated to the Islamic State. Investigations established that Rachel's credit card had been used to buy bitcoins and the trail linked the fraud to individuals within the Islamic State affiliate in Somalia. Fatima Patel, Sayfudeen Aslam del Vecchio and Mussa Ahmad Jackson were accused of this murder; encrpyted communications between the accused indicated their desire to carry out a terrorist attack. A particular message sent on 9 February 2018, allegedly indicated that they were planning to "kill the kuffar (reference to non-Muslims) and abduct their allies, to destroy infrastructure and to put fear in the heart of the kuffar".[94]

Secure, anonymous transactions and deep web transactions such as purchasing weapons, tools or other illicit goods while maintaining anonymity is a tactic that terrorists are likely to use. Unmoderated social media allows development of networks of content and contacts that are decentralised, built on blockchain technology and not owned by any company thus no one has responsibility to moderate. [95]

5-7 Cyber Tools

Cyber tools necessary for hacking, the deployment of malware, and other forms of digital attack have become a weapon of choice for criminals, both organised and lone-wolf criminals. The targeting of cyber

---

[92] FATF REPORT (2023) Crowdfunding for Terrorism Financing https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

[93] TRM, Terrorism financing: six related cyrpto-trends to watch in 2023 (2023) https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023

[94] BBC, Rodney Saunders: South Africa identifies body of missing horticulturalist (2018) https://www.bbc.com/news/world-africa-43901056

[95] n. 93

infrastructure, stealing sensitive information and disruption of communications (hacking of government websites, spreading ransomware, or orchestrating distributed denial-of-service (DDoS) attacks) are on the rise. Software on demand has been used to develop independent chat apps, online forums, document sharing apps, or other platforms.[96] One of the most prominent cases of hacking by terrorists is the 2015 Ardit Ferizi, or "Th3Dir3ctorY" case whereby a hacker accessed servers in the US and extracted personally identifiable information of approximately 1,300 United States military and government personnel. He later contacted IS members through Twitter and Skype and handed over the information to the "Islamic State Hacking Division," who published the data.[97] In another case in 2022, the pro-Da'esh cyber security capability "Electronic Horizon Foundation" released a short instructional video via their dark website and social media channels about "Locker," a smartphone security capability that would automatically erase all data after several unsuccessful attempts to unlock the device. This was shared with its affilitates through the encrypted chats.[98]

Other forms of technology that terrorists are likely to exploit include Virtual Reality (Vr) / Augmented Reality (Ar). These immersive experiences allow for improved training through provision of realistic training simulations for recruits. They also increase chances of radicalization through immersive environments for indoctrination. New recruits are also likely to be engaged through interactive experiences or new forms of social media. Gaming has been used to disguise recruitment and radicalisation content. For instance, the livestream attacker footage of the Christchurch attacks in 2019, was overlaid with "minions" cartoon character images over the victims to evade detection and gamify the attack.[99] This dangerous trend targets the youth that spend a lot of time online, radicalising

[96] n. 68

[97] Archives of US Department of Justice, ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison (2016)

[98] Cyber & Terrorism Jihad Hub, Pro-ISIS outlet releases video guide on installing, using 'Locker' phone data erasing app (2022) https://www.memri.org/cjlab/pro-isis-outlet-releases-video-guide-installing-using-locker-phone-data-erasing-app

[99] Geneva Internet Forum, AI & violent extremism (2025) https://dig.watch/topics/violent-extremism.

them into thinking that killing other people is a game. This is a tactic likely to be picked by bigger terrorist groups to target youthful recruits.

Autonomous driving vehicles are already in production, and can be easily used by terrorists as vehicle-borne explosive devices. Indeed, the January 2025 explosion of a Tesla Cybertruck outside of the Trump Hotel in Las Vegas, US brought fear that terrorists might exploit autonomous driving vehicles for terrorist attacks, particularly in light of the increased usage by IS of van and car rammings into crowded areas.[100]

6. Conclusion

From the foregoing, it is obvious that terrorists will benefit from technology just like everybody else. It is also imperative to note that the improvement that technology brings to security will benefit security agents to deal with terrorism, with enhanced surveillance tools, big data analytics and Machine Learning. As far as surveillance and targeting by extremists is concerned, advanced computer vision and NLP can improve the ability to monitor, identify, and target individuals or groups of interest.

Major concerns persist on the issues of content moderation circumvention and an increase in propaganda and disinformation disguised as games, through the modification of existing online games or creation of new online game-play spaces, thus allowing for passage of increasingly compelling propaganda.[101]

That said, it is noteworthy that the Global North has been more successful at calling out tech companies after incidents such as the 2019 Christchurch, New Zealand attack. However, there has been much less consumer pressure across Africa, possibly because of the 'digital divide', competing policy priorities and a relative lack of awareness on the continent.

---

[100] The Guardian, One dead after Tesla Cybertruck explodes outside Trump hotel in Las Vegas (2025) https://www.theguardian.com/us-news/2025/jan/01/tesla-truck-fire-trump-hotel-las-vegas

[101] n. 99

However, to reduce the advantage that terrorists would have from technology, some short term, mid term and long term measures should be considered. In the short term, governments need to partner with tech companies to detect and remove extremist content online. Already, governments in partnership with tech companies are identifying the risks and exploring solutions, such as attempting to 'jailbreak' Generative AI models mimicking how bad actors might try to circumvent safety efforts. Jailbreaking is a terminology used to describe ways of tricking or guiding the chatbot to provide outputs that are intended to be restricted by the LLM's internal governance and ethics policies.[102] Tech companies are also employing experts who can help them seal loopholes used for nefarious purposes.

It is also imperative that security agents are trained on digital forensics, exploitation of the open sources and social media monitoring. To curb use of virtual assets for terrorism financing, mobile money and cryptocurrencies should be regulated.

Since technology is cross-cutting, and the terrorist groups in Africa are traversing regions, it is prudent to establish regional cyber intelligence and defence centres for liaison and collaboration. In addition, governments need to partner with non-state actors such as religious leaders and civil society organisations to carry out credible counter and alternative narratives and amplify them in the online spaces. There is also need for generation of content moderation tools in African languages, and also create African databases that AI models can trained on, to reflect the realities in the terrorism-prone areas.

In the long term and for sustainability, there is need for national and regional cyber security legal and policy frameworks. There also need to promote digital literacy and resilience amongst local communities.

References

[102] n.99.

Abass, H. (2025). Artificial Intelligence in Cybersecurity: Advancements and Challenges in Data Protection. *Bilad Alrafidain Journal for Engineering Science and Technology*, *4*(2), 13-27.

ACLED, Cabo-Ligado update 5-18 May (2025) https://acleddata.com/update/cabo-ligado-update-5-18-may-2025

Afriyie, F. A. (2023). A tale of two jihads: Unraveling the atrocities of Islamic State in the Greater Sahara (ISGS) and Jama'at Nasr al-Islam wal Muslimin (JNIM) in the Sahel. *Austral: Brazilian Journal of Strategy & International Relations, 12*(23).

Aguilera, A. (2023, July 5). Drone use by violent extremist organisations in Africa: The case of Al-Shabaab. *GNET Insights.* https://gnet-research.org/2023/07/05/drone-use-by-violent-extremist-organisations-in-africa-a-case-study-of-al-shabaab/

Aina, F., & Ojo, J. S. (2023). The "webification" of jihadism: Trends in the use of online platforms, before and after attacks by violent extremists in Nigeria.

Ajiboye, B. M. (2022). Boko Haram: Shekau's Demise–Halcyon or Nadir for Sub-Saharan Africa's Fight Against Terrorism?'. *Conflict Studies Quarterly*, *41*, 3-14.

Allen K.(2021). Drones and Violent Non-State Actors in Africa. ACSS, https://africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/.

Allen, K. (2025). Unmanned aerial systems and violent non-state actors in Africa: Proliferation, adaptation and use. In *Drones in the African battlespaces* (pp. 125–145). Springer Nature Switzerland.

Ayad, M. (2025). Teenage Terrorists and the Digital Ecosystem of the Islamic State. *CTC Sentinel*, *18*(2), 1-8.

Ojo, J. S. (2024). *Convergence of Terror: Boko Haram Insurgency, Fulani Militancy, Armed Banditry, and Separatist Movement in Nigeria* (Doctoral dissertation, Doctoral dissertation, University of Portsmouth).

Bacon, T., & Doctor, A. C. (2023). The death of Bilal al-Sudani and its impact on Islamic State operations. *Nexus.*

Badurdeen, F. A. (2023). Al-Shabaab Financing: Sources, Methods, and Countering terrorist Financing. In *Countering Terrorist and Criminal Financing* (pp. 483-496). CRC Press.

Barkindo, A. (2023). Boko Haram-ISWAP and the Growing Footprint of Islamic State (IS) in Africa. *Counter Terrorist Trends and Analyses*, *15*(2), 12-17.

Bukarti, B., & Munasinghe, S. (2020). The Mozambique conflict and deteriorating security situation. *Tony Blair Institute for Global Change*, *19*.

Bolmvall, N. (2025). Explaining Violence: A qualitative case-study of the ADF's rebel violence against civilians. www.diva-portal.org

Daily Maverick. (2022, March 14). Red-flagged terror-linked networks in South Africa: A ticking time bomb. https://www.dailymaverick.co.za/article/2022-03-14-red-flagged-terror-linked-networks-in-south-africa-a-ticking-time-bomb/

Demirtaş, T., & Warsame, A. A. (2025). Al-Shabab's evolving media strategy: Narratives, tools, and impact (2006–2025). *SETA.*

EU Agency for Asylum, (2025) Analysis based on ACLED data: Somalia. https://euaa.europa.eu/publications/asylum-report-2025EUAA, 2025.

Europol. (2023, March 27). Criminal use of ChatGPT: A cautionary tale about large language models. *Europol Newsroom.* https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models

Ezra, M. (2025). Central Sahel: An equation of crises for a sum of paradoxes. *The African Geopolitical Atlas 2025: Conflicting Information, Conflicted Realities.*

Global Terrorism Index. (2025). *Global Terrorism Index 2025.* Institute for Economics & Peace. https://reliefweb.int/report/world/global-terrorism-index-2025

Guhad, H. A. (2025). Terrorism in Mozambique: Evolution, context, and prognosis. In *Palgrave Handbook of Terrorism in Africa* (pp. 519–538). Springer Nature Switzerland.

Harper, M. (2019). Is anybody listening? Al-Shabaab's communications. In M. Keating & M. Waldman (Eds.), *War and peace in Somalia: National grievances, local conflict and Al-Shabaab.* Oxford University Press.

ICCT. (2025). *The Islamic State in 2025: An evolving threat.* International Centre for Counter-Terrorism.

Institute for Security Studies, (2025). Lake Chad Basin: Insurgents Raise the Stakes with Weaponised Drones. issafrica.org, https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones.

Iyekekpolo, W. O. (2016). Boko Haram: Understanding the context. *Third World Quarterly, 37*(12), 2211–2228.

Johns, A., Matamoros-Fernández, A., & Baulch, E. (2023). *WhatsApp: From a one-to-one messaging app to a global communication platform*. John Wiley & Sons.

Joseph, D., & Maruf, H. (2018). *Inside Al-Shabaab: The secret history of Al-Qaeda's most powerful ally.* Indiana University Press.

Kellar, K. R. (2024). Examining the Factors that Contribute to the Survival and Resilience of the Al-Shabaab Terrorist Organization. https://academicworks.cuny.edu/gc_etds/5776/

Kelly, F. (2019). Islamic State enforced leadership change in West Africa Province, audio reveals. *The Defense Post.* https://www.thedefensepost.com/2019/03/15

Kelly, F. (2019, August 1). ISWAP killed 'dozens' of Nigeria and Chad troops near Baga in July 29 clashes. *The Defense Post.* https://www.thedefensepost.com/2019/08/01

Liang, C. S. (2022). Technology and terror: The new arsenal of anarchy. In *Handbook of Security Science* (pp. 1–24). Springer, Cham.

Maruuf, H. (2024). Inside Somalia's war on al-Shabab disinformation. *VOA News.* https://www.voanews.com/a/inside-somalia-s-war-on-al-shabab-disinformation/7528211.html

McSwiney, J. (2025). Democratic Resilience in Retreat: Australia's Response to the 2002 Bali Bombings. *Political Studies Review*, 14789299251360661.

Meyer, A., Simonet, L., & Späth, J. (2025). The European Union and the Sahel: The day after. https://www.ssoar.info/ssoar/bitstream/handle/document/99531/ssoar-2025-meyer_et_al-The_European_Union_and_the.pdf?sequence=1&isAllowed=y

Military Africa,(2025). Africa's Insurgents and Terrorists Are Adopting Drones, militaryafrica.com, February 23, 2025 https://www.military. africa/2025/02/the-rise-of-drone-warfare-insurgents-and-terrorists-in-africa/

Mwale, B. (2025). The regulation of terrorist online content in Africa: an overview of the applicable regional instruments and the legal frameworks of South Africa, Kenya and Nigeria. *Journal of Policing, Intelligence and Counter Terrorism*, 1-18.

Nsaibia, H. (2024). Newly restructured Islamic State Sahel aims at regional expansion. *ACLED.* https://acleddata.com

Pack, J., Smith, R., & Mezran, K. (2022). *Origins and evolution of ISIS in Libya*. *Atlantic Council.*

Parale, Yogesh. (2023). Analyzing the Rhetoric Posed by the ISKP in Afghanistan: A Case Study of the Voice of Khorasan. *Indian Journal of Asian Affairs* 36, no. 1/2: 41–54. https://www.jstor.org/stable/27307174.

Reuters. (2025, January 1). Musk says Tesla investigating Cybertruck fire in Las Vegas. *Reuters.* https://www.reuters.com/business/autos-transportation/musk-says-tesla-investigating-cybertruck-fire-las-vegas-2025-01-01/

Schweitzer, Y., & Avita, S. (2022). Jihadi war in Sinai. *Institute for National Security Studies (INSS).*

Security Council Report. (2025, August). UN Office for West Africa and the Sahel (UNOWAS). *Monthly Forecast.* https://www.securitycouncilreport.org/monthly-forecast/2025-08/un-office-for-west-africa-and-the-sahel-unowas.php

Sergie, M. A., & Johnson, T. (2015). Boko Haram. *Council on Foreign Relations*, *7*..

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12), 324.

Svicevic, M. (2024). The SADC mission in Mozambique. *Mozambique's Cabo Delgado Conflict: International Humanitarian Law and Regional Security*.

Thurston, A. (2020). *Jihadists of North Africa and the Sahel: Local Politics and Rebel Groups*. Cambridge University Press.

Tripathi, D. (2011). *Breeding ground: Afghanistan and the origins of Islamist terrorism.* Potomac Books, Inc.

Tripodi, S. (2025). Explaining the resilience of insurgent organisations using a four-function paradigm: The case of Jama'at Nusrat Al-Islam wal Muslimin (JNIM). https://dspace.cuni.cz/handle/20.500.11956/201308

Tufekci, Z. (2018). How social media took us from Tahrir Square to Donald Trump. *MIT Technology Review, 14*(18).

Ukaeje, O. (2025). State and the terrorist threats in Chad. In *Palgrave Handbook of Terrorism in Africa* (pp. 83–107). Springer Nature Switzerland.

UN Analytical Support & Sanctions Monitoring Team. (2025). *35th–36th reports on ISIL/al-Qaida. https://docs.un.org/en/S/2025/71*

United Nations Panel of Experts on the DRC Security Council, S/2021/560, Annex 14, https://documents.un.org/doc/undoc/gen/n24/373/37/pdf/n2437337.pdf

VOA News. (2024, October 18). Uganda captures rebel bomb expert in eastern DRC. *VOA Africa.* https://www.voaafrica.com/a/uganda-captures-rebel-bomb-expert-in-eastern-drc-/7618180.html

Warner, J., & Weiss, C. (2017). A legitimate challenger? Assessing the rivalry between al-Shabaab and the Islamic State in Somalia. *CTC Sentinel, 10*(10), 27–32.

Weeraratne, S., & Recker, S. (2018). The isolated Islamists: The case of the Allied Democratic Forces in the Ugandan–Congolese borderland. *Terrorism and Political Violence, 30*(1), 22–46.

Williams P., The Somali National Army Versus al-Shabaab: A Net Assessment (2024) CTC Sentinel 17(4). *https://ctc.westpoint.edu/the-somali-national-army-versus-al-shabaab-a-net-assessment/*

Zelin, AY. (2024). New issue of the Islamic State's newsletter: *al-Nabā* #437. *Jihadology.* https://jihadology.net