

Artificial Intelligence and Asymmetrical Power in African Conflicts:
Mozambique and Ahlu Sunnah wa-Jama'a

Ethan Huffaker

A Thesis in the Field of International Relations
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

November 2026

Abstract

This thesis examines how artificial intelligence is beginning to reshape conflict, and information ecosystems in Africa, with a particular focus on Mozambique. While much of the global literature on AI and security is centered on highly digitized environments, this study argues that AI can also affect low-connectivity conflict zones through uneven, and indirect forms of adoption. Using the conflict of Ahlu Sunnah wa-Jama'a in Mozambique's northern state, Cabo Delgado, as a case study, this thesis explores how insurgent groups and state institutions interact within an asymmetrical technological environment that arises from weak governance, limited intelligence sharing, political tension and overall digital abstinence. Focus is given to propaganda from generative AI, algorithmic amplification for controversial media, the role of WhatsApp vs traditional social media apps in Africa, and the current limitations of data and research in Mozambique. The findings suggest that AI in African conflict does not depend on widespread access to advanced tool, but rather how technologies intersect with fragile state control and uneven cooperation in the region. It concludes that AI is likely to deepen existing asymmetries in conflict environments where corruptive governments struggle to respond as quickly as insurgent movements and actors can adapt.

Frontispiece

I was just a young missionary living abroad in Mozambique when a young girl approached me and my companion. At the time, I was early in the process of learning Portuguese, so I struggled to understand most of the conversation. After a few minutes, the room grew heavy and I attempted to understand as much as I could as she tried to speak behind her tears, but as we walked away, I asked my native speaking companion if he could translate.

When she was still a teenager, she grew sick one afternoon and required medical attention. Her hospital bills were too high for her struggling family, and her mom lost her temper when she was required to pick up a prescription. A huge argument broke out, which resulted in her being kicked out. After a few days, her mom called, apologized and begged her to come home.

The next day, when she arrived, her mother was standing in the living room with two unknown men. She tried to struggle but was knocked out during the chaos. When she came around, she realized she was locked in a room and chained to a wall alongside another girl her age. For what she estimates was a few weeks, maybe a month, she was raped, denied food and water and eventually left for dead in a nearby cave before she was found by a kid who was playing nearby. All she wanted to know from us missionaries was how she could find happiness again in a screwed-up world. I have sought to help end human trafficking and terrorism ever since.

Author's Biographical Sketch

Ethan Huffaker is a graduate student at Harvard University specializing in international relations, with a focus on African security, conflict, and emerging technologies. His research explores the intersection of artificial intelligence, terrorism, propaganda, and information ecosystems in sub-Saharan Africa, with particular emphasis on Mozambique. He served a two-year LDS mission in Mozambique, an experience that deepened his regional knowledge and informed his academic and professional interests.

In addition to his academic work, he previously founded a nonprofit organization dedicated to supporting victims of human trafficking in Africa and has participated in humanitarian work in Brazil, Belize, Nepal, and Cape Verde. Drawing on regional experience and Portuguese language proficiency, his work examines how technological change is reshaping conflict dynamics, state responses, and transnational security challenges.

Dedication

To the parents who sent me to Brazil when I was only 16 to
help families who lost their homes in a mudslide.

Thank you for letting me learn firsthand how big and small
the world is at the same time.

Acknowledgments

I would like to publicly thank my thesis director, Harry Bastermajian, as well as my research advisor, Doug Bond, for guiding me through the rigorous process of academic writing and research. Professor Bond was a key contributor to my overall success at Harvard and a mentor in my African studies, and I was fortunate to have him as a professor for three separate courses during my time as a student.

I am also grateful to the faculty and staff of the International Relations program at Harvard University for providing the academic environment and financial resources that enabled me to pursue this research.

Finally, I wish to express my deepest gratitude to my family and friends for their unwavering support and encouragement throughout this journey. Those closest to me know that I consider Africa to be my second home, and it is my hope that this research, in some small way, may contribute to a safer and more promising future for those entrusted with its care.

Table of Contents

Frontispiece	iv
Author's Biographical Sketch	v
Dedication	vi
Acknowledgments	vii
List of Figures	x
Chapter I. Introduction.....	1
Use of AI for Terrorism	3
Definitions.....	7
Chapter II Literature Review	11
Types of Artificial Intelligence	11
Broader Implications	13
AI Hallucinations and Social Instability	14
Terrorist Gen AI Adoption.....	16
Uneven Research.....	20
Chapter III. Case Study.....	21
Origins and Identity of Ahlu Sunnah wa-Jama'a.....	21
Algorithmic Amplification	23
Spillover, Displacement and AI-Enabled Translation	25
Geopolitical Pressure	28

Corruption in LNG Project Development	29
Intelligence Failures	31
Generative AI in African Contexts	34
The Role of WhatsApp	37
Chapter IV: Analysis and Discussion	40
Uneven Technological Adoption	40
Evidentiary and Attribution Problems	42
Asymmetrical Power Dynamics.....	44
Public Policy Implications	45
Future Risks and Jailbreaking	46
Broader Implications for Africa.....	47
Chapter V. Conclusion.....	49
Appendix. Figures and Maps	51
References.....	57

List of Figures

Figure 1 .The Nexus of AI Terrorism	51
Figure 2. Recorded Incidents of UASs’ Use by NSAGs in Africa	52
Figure 3. Types of Use of UAS by NSAGs in Africa, January 2018–June 2023	53
Figure 4. Map of Displacements in Cabo Delgado	54
Figure 5. List of Indigenous Languages Spoken in Mozambique	55
Figure 6. Gender Disparity in Internet Use, Mozambique & Other African Countries.....	56

Chapter I.

Introduction

“There is an urgent need for more research to understand the impact of AI on society and to take steps to mitigate its potential risks.”

—Kate Crawford

Few terms inspire as much intrigue as artificial intelligence (AI), a concept that simultaneously stirs fear, sparks hope for the future and cloaks itself in an enigmatic veil. A large range of potential emotions stems from the fact that the technology underlying AI is evolving at an unprecedented pace in human history, making its potential, as well as its limitations, appear virtually boundless. This unstoppable evolution forces consumers, scholars, and lawmakers of AI to find themselves caught in a kind of paradox akin to a technological revolving door: the moment one aspect of AI is understood and mastered, it shifts again, forcing the learner to re-enter the cycle and adapt anew. Although the technological output itself is ever-changing and evolving, there are still key distinctions that make the idea of AI less daunting, especially for policymakers and governments, and may allow everyone to finally exit the metaphorical revolving door by gaining an understanding of the five pillars that form AI technology: data dependence, human design and oversight, the goal of simulation, algorithmic foundations, and dual potential.

However, simply understanding the core concepts of AI will not change how the battlefield over technology has evolved through the widespread release of these models, and how the world has transformed into an asymmetrical power shift like the adaptation

of nuclear deterrence strategy following the end of World War II. Nuclear deterrence, as defined by the Carnegie Council for Ethics in International Affairs, “refers to a principle in international relations where the retaliatory potential and destructive force of nuclear weapons prevent nations from launching a nuclear attack.”¹ Nuclear deterrence, in theory, works in asymmetrical power struggles because the fear of how one nuclear warhead could be used is often enough to lead to negotiations. If, for example, any nonstate actor or terrorist group possessed solely one warhead, the fear of where that one device would be used is often sufficient to deter full out nuclear war. Although the literal kinetic consequences of AI usage versus a nuclear bomb remain significantly different, they both possess a similar shadow that looms over lawmakers and militaries around the world, which is fear through the means of distributed equal strength and retaliation power to nonstate actors.

Although comparing AI to nuclear deterrence may sound extreme to some, AI has already taken over various forms of warfare that began at the start of this decade. Vladimir Putin, the longstanding President of Russia, has been a strong advocate for the military uses of AI and has gone on the record stating: “Whoever becomes the leader in this sphere will become the ruler of the world,” (when referencing the power of artificial intelligence.)² At the heart of current AI warfare, one of the most frightening tools are drones that are specifically designed to attack remote targets by becoming something similar to a kamikaze weapon:

Reports now suggest that Russian forces have also used KUB loitering munitions in Kyiv. According to their

¹ Carnegie Council for Ethics in International Affairs, “*Nuclear Deterrence*,” Ethics & International Affairs, accessed September 5, 2025

² Radina Gigova. “*Who Vladimir Putin Thinks Will Rule the World.*” CNN, September 2, 2017.

manufacturer ZALA AERO, these are “high-precision” small-size weapons designed to destroy remote targets and have the potential to “deliver a special load to the target coordinates, which are set manually or on the image from the guidance system”, presumably a preloaded data set.³

Use of AI for Terrorism

AI driven drone attacks did not begin with the Russian/Ukraine war (and they will certainly not end there) as many terrorists’ organizations have begun operating drones across Africa several years prior. One example is when the extremist group, Ahlu Sunna wal-Jama’a, (ASWJ) in Mozambique began to utilize UAS (uncrewed aerial systems) to coordinate planned attacks dating back to as early as the 2020’s. The UAS’s were used to gather intelligence for targeting potential victims and included several reported instances and attacks at various locations, such as a police station near the Nampula airport.⁴ In a report given by the UNIDIR in a series titled “*The Use of Uncrewed Systems by Non-State Armed Groups*” they state that across Africa, 43% of terrorist group UAS activities are for gathering intelligence and planning, whereas only 11% are for direct and/or indirect attacks. (Refer to figure 1 to see total recorded UAS incidents in Africa from 2018-2023, and figure 2 which shows a breakdown of why those UAS incidents were used.)⁵

The real danger in AI is not from the existence of drones itself, but rather the accelerated speed at which systems can process data without the risk of human presence.

³ Ingvild Bode and Anna Nadibaidze, “*AI and Drones in the Russian Invasion of Ukraine: Challenging the Expectations?*,” *AutoNorms*

⁴ Bárbara Morais Figueiredo, “*The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa*”. Geneva: United Nations Institute for Disarmament Research, 2024

⁵ Bárbara Morais Figueiredo, “*The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa*”.

AI is different from other technologies due to the algorithmic functions designed to mimic human interaction. With proper governance, it can often achieve desired results and make certain aspects of life and work relatively easier for many individuals. Without governance, however, it can, and has already in several instances, may harm human society, as we can see with the existence of UAS attacks.

As mentioned before, artificial Intelligence is made up of five core elements; data dependence, human design (and oversight), goal of simulation (the purpose behind its creation), algorithmic foundations which are designed to mimic how a human would react or respond, and finally “dual potential”, or the ability to be used in various ways. AI simply contains more components than other types of technologies, which in consequence translates to more ways to sidestep and abuse the system. Since all five elements must be handled with care, a nonstate actor or terrorist group simply needs to overcome one aspect and then it can become a tool for violent purposes rather quickly.

Unfortunately, there are various ways that terrorist groups and nonstate actors can utilize artificial intelligence to achieve their goals of disrupting economies for financial and personal gain. Although often facilitated from lack of proper governance, nonstate actors can use AI to create powerful deepfakes, design catfish profiles to lure in potential victims, cover financial tracks through complex crypto algorithms, monitor social media to generate large dataset tokens, and lastly impact political elections by spreading fake images and propaganda through the generation of false media; all at lightning speed.

One common way in which terrorist groups utilize technology software is from a term that was widely adapted following the release of the iPhone: a process known as “jailbreaking”. When a device is jailbroken, it essentially shuts down or removes certain

barricades and walls that are put in place to protect consumers, as well as hinder illegal activities. Many readers might remember the age of the first iPhone and iPod touch when jailbroken users could circumvent the entire apple store and download any app they wanted for free without paying for access.

Looking at reports compiled by academics and federal organizations, there is not a substantial amount of research to support the idea that terrorist groups have discovered ways to jailbreak complex AI models and software to such a high extent just yet. However, none-state actors have continued using AI to achieve “workarounds” to accomplish the same final product as if it had been jailbroken. For example, with many legal safe barriers in place, terrorist groups cannot simply type a prompt and ask for an image of a political leader doing something illegal. However, they can use generative AI to make multiple images, and then simply stack them on top of each other using basic editing software to achieve the same misleading effect, such as when pictures of babies and children had been manipulated with AI during the war in Gaza.⁶

However, it is only a matter of time until jailbroken models have become more normalized, as technology becomes more accessible and less expensive. Some examples of what current AI models can accomplish when utilized by a nonstate actor includes, but is not limited to: sidestepping paywalls, granting the user the ability to generate misleading political photos or images of political leaders, (such as this example of Al-Qaeda propaganda made in 2023)⁷ generating graphic or mature rated images of civilians or children, attempting to access personal or private data from deep searches, or using

⁶ Clarisa Nelu. “*Exploitation of Generative AI by Terrorist Groups.*” International Centre for Counter-Terrorism (ICCT), June 10, 2024.

⁷ Tech Against Terrorism. *Early Terrorist Experimentation with Generative Artificial Intelligence Services.* Briefing, November 2023.

various techniques in an attempt to avoid financial crime detection by hiding complex money flow through cryptocurrency transactions.

African contexts are of particular interest, as artificial intelligence use seems to generate an asymmetrical power shift that can favor nonstate actors. In many cases, such as the attacks by Ahlu Sunnah wa-Jama'a in Cabo Delgado, Mozambique, these groups do not need to utilize the full technological power or models that are available in order to achieve meaningful advantages. Instead, they can adopt accessible and cheaper models to generate propaganda campaigns and perform surveillance while state institutions often struggle with basic infrastructure, intelligence coordination with neighboring countries and their own corruption scandals. As a result, even modest forms of AI technology can have disproportionate effects that allow nonstate actors to exploit wide governance gaps that result in deadly outcomes.

This thesis focuses on three major components: the first is defining various ways African terrorist groups use AI, such as utilizing deepfakes to spread propaganda and the usage of UAS. The second is analyzing one large case study; the terrorist attacks and growth of Ahlu Sunnah wa-Jama'a in Mozambique that began in 2017, and how AI has played a role. The final part of the thesis discusses lack of intelligence and research on AI and its connection to terrorism, political election tempering, and how in African contexts AI is creating an asymmetrical power dynamic.

Definitions

Ahlu Sunnah wa-Jama'a (AWSJ): Extremist group primarily in the state of Cabo Delgado Mozambique that surfaced in the 2010's. Also has been called al-Shabaab by local Mozambicans.

Artificial Intelligence (AI): Computer systems designed to perform tasks that normally require human intelligence. Umbrella term for discussing several versions of AI.

Machine Learning: Subset of artificial intelligence where systems learn patterns from large sets of data to make predictions.

Generative AI: AI models designed to create new content, often in forms of images, audio, video or code, from patterns learned from large training datasets. Its main purpose is generating new content to resemble human-created material.

AI Agents: AI models designed to act without human intervention, to pursue goals and complete tasks. Customer chatbots are forms of AI agents.

Hallucinations in AI agents: Fake, misleading or biased information generated by an AI model, but presented as truth or factually correct to the user. AI hallucinations often exacerbate confirmation bias by showing users what it thinks they want to see.

Algorithm / Algorithmic Amplification: Pre-programmed rules for online engagement systems to show users content they are most likely to engage with based on previous historical online activity.

Filter Bubbles: Personalized online environments where users are shown bias content that specifically aligns with prior interests and behaviors.

Sextortion: A form of exploitation where the scammer will use someone's sexual images, videos or record conversations to blackmail, threaten, manipulate and coerce an individual into paying them.

Deepfake Sextortion: A form of sextortion, where artificial intelligence is used to generate fake images, audio or videos of an individual using generative artificial intelligence models and then using that material to blackmail an individual.

Mini-Personalized Machine Learning Models: Theoretical small-scale data-driven systems built from smaller datasets to identify patterns among a specific group or individual, to be tailored for propaganda and recruitment purposes by non-state actors and terrorist groups.

Non-State Actors: Individuals or organizations that operate outside formally controlled or recognized government but can still impact political and military outcomes.

Insurgency: Organized rebellion against a state or government, typically involving violence to pursue a political objective.

Terrorist Affiliate: A group formally (or informally) connected to a larger terrorist organization through shared ideology and sometimes operational support. Usually consists of smaller groups that operate in more localized locations.

Spillover Effect: The spread of violence and instability from an active conflict zone into a neighboring state or country. This can often include fighters and terrorist groups attacking across border lines to control transport routes in and out of a conflict zone.

State Fragility: When a state or government lacks the strength or capacity to effectively govern or deliver basic public services, such as transportation. Fragile states are more likely to be targeted by nonstate actors and terrorist groups.

Forced Displacement: Occurs when individuals or whole communities are compelled to flee due to violence and/or natural disaster. Displacement, whether forced or not, increases vulnerability for individuals.

Forced Recruitment: Coercive enlistment into terrorist groups or criminal organizations through threats and blackmail and often succeeds from a lack of other viable alternatives for the individual. More common in conflict zones.

Election Interference: Deliberate effort to manipulate and undermine the integrity of an election through various forms of disruption. Includes, but is not limited to, disinformation, propaganda, ballot tampering, cyber manipulation, riots and protests, and blackmail.

Propaganda: Creation and distribution of information designed to sway or manipulate public opinion. Well often emotionally charged, can also include images, videos and text designed to spread false or extremely bias information.

Disinformation: False information that is distributed to an audience. Unlike misinformation, which may be spread unknowingly, disinformation is inaccurate information spread with the goal to manipulate its audience.

Social Media Bots: Automated accounts designed to post, share, interact or amplify content online. Often used to spread propaganda or disinformation.

End-to-End Encryption: Communication security method that allows only the user and recipient to read contents of a message. End-to-end prevents even the hosting platform from accessing information in most cases.

WhatsApp: Social media platform owned by META that allows grants end-to-end encryption and is very popular in most places in Africa due to its free cost.

FADM: Armed Forces for the Defense of Mozambique is the official recognized national security for the defense of Mozambique.

FISMA: requires federal agencies, including CMS, to establish comprehensive information security programs.

Chapter II

Literature Review

Recent literature on artificial intelligence in Africa emphasizes that AI is not a singular tool, but a category that consists of distinct models which includes three main types: machine learning, generative AI and AI agents. Understanding how these models differ is important in the African context, where their applications may intersect with terrorism and human trafficking, but still differing significantly in function and operational usage.

Types of Artificial Intelligence

To begin understanding how artificial intelligence is applied in African contexts, the first step should be examining machine learning models (MLM) that track and compile very large data sets (often called tokens of data) for customized reasons. One more well known example of how machine learning models are being used, is in the modern medicine sector where physicians are utilizing machine learning AI to teach computer systems what to screen for in x-rays, in hopes to be able to spot early signs of cancer.⁸ In order to perform these type of detective functions at an effective rate, the AI model must research and analyze millions of versions of x-rays to be able to recognize the difference between no cancer, early cancer and mid-late stages of cancer. It is not uncommon for machine learning models to review millions, billions and even trillions of tokens

⁸ Alan Zeichick. “*AI vs. GenAI vs. ML: Key Differences.*” Oracle, May 9, 2025.

of data to be able to do their jobs effectively.⁹ In a report released just last year, over 200,000 terrorist attacks were analyzed using an artificial intelligence MLM to track and predict terrorist attacks across the globe with many instances occurring in various regions across Africa, which showed that a “hybrid feature selection reported an accuracy of 97.81% in predicting the danger zones.”¹⁰

Generative AI (most often referred to as gen AI) is when a model takes large tokens of data and compiles a library with the capacity to “generate” new content in the way a that mimic what a human creates. Using our previous x-ray example, gen AI would be when a model generates a picture of what an x-ray might look using an “estimate” of previous data it has examined, to then create the x-ray as if it was created by human. So, while machine learning attempts to predict or analyze in real time, gen AI creates an image/video/audio set based on the closest version compared to the tokens it has been trained on. Published research on generated AI content shows various instances where nonstate actors that operate in African countries have generated false and misleading images to impact elections¹¹. However, research documenting instances where gen AI was aimed specifically at African audiences from terrorists organizations is more limited.

⁹ Adam Ibrahim, Benjamin Thérien, Kshitij Gupta, Mats L. Richter, Quentin Anthony, Timothée Lesort, Eugene Belilovsky, and Irina Rish. “Simple and Scalable Strategies to Continually Pre-train Large Language Models.” *Transactions on Machine Learning Research*, June 2024.

¹⁰ Ume Kalsooma, Sahar Arshad, Amerah Albarah, Imran Siddiqi, Saeed Ullah, Abdul Mateen, and Farhan Amin. “A Big Data Driven Multilevel Deep Learning Framework for Predicting Terrorist Attacks.” *Scientific Reports* 15 (2025): Article 23060.

¹¹ Gregory Gondwe, “AI-Driven Disinformation and Political Influence on WhatsApp in South Africa’s 2024 Elections,” *The International Journal of Press/Politics* (November 2025): 1–20

One such example occurred in June 2023, when “OSINT analysts identified an al-Qaeda (AQ) aligned media entity using what appears to be generative AI for propaganda production.”¹² Spotting well produced generative AI is a skill in of itself, but often small details tend to leak through. In the same report given by the OSINT, the images associated with the al-Qaeda group contained various inconsistencies, such as a “bent barrel” or improper placement of flags on uniforms that would often get overlooked to the untrained eye.¹³

AI agents are more niche in their utilization and used to export mundane tasks, often with the goal of saving time/money, while also appearing and acting like a real human. Many large corporations have created AI costumer service agents to assist and answer routine questions, but AI agents are usually only trained on the data pertinent to their jobs/companies. In addition, what sets AI agents apart is their ability to act, or perform real functions, such as processing an online refund or changing a user’s flight schedule, without requiring direct human intervention by the company or organization it represents.

Broader Implications

Even when branching outside of Africa, specific research on terrorist groups utilizing interactive artificial intelligence technology (such as chatbots) when compared to generative AI is much lower. AI is a newer technology which only became mainstream this last decade and although research is evolving every

¹² Tech Against Terrorism, *Early Terrorist Experimentation with Generative Artificial Intelligence Services*, briefing, November 2023

¹³ Tech Against Terrorism, *Early Terrorist Experimentation with Generative Artificial Intelligence Services*, briefing, November 2023

day, the pace to match its use may prove rather strenuous. Over the last few years, chatbots have almost certainly brought an influx in usage by nonstate actors. Research indicates that chatbots are an attractive avenue for these insurgent groups, because children who are suffering from abuse and depression are increasingly turning to chatbots for comfort, which aligns with traits of vulnerability that extremist groups have historically exploited.¹⁴

AI Hallucinations and Social Instability

However, AI models are not void of potential negative consequences and can often suffer from “hallucinations” or the inability to follow complex instructions, therefore generating false or irrelevant prompts and outputs.¹⁵ Emerging research into AI hallucinations is quite strong, which emphasizes four large areas of conflict as a result: social misinformation, public trust, professional and intuitional harm, and legal and governing issues in their relation to something known as the “accuracy paradox”.

Before the creation of AI, researchers could study human intent as a primary basis for analyzing misinformation that occurs online. However, since AI models often combine complex data configuration from billions of tokens, misinformation can generate from a variety of means, such as receiving improper training data, bugs and technical issues, human programmers, or even something

¹⁴ Clarisa Nelu. “*Exploitation of Generative AI by Terrorist Groups.*” *International Centre for Counter-Terrorism (ICCT)*, June 10, 2024

¹⁵ Xu Huang, Weiwen Liu, Xiaolong Chen, Xingmei Wang, Hao Wang, Defu Lian, Yasheng Wang, Ruiming Tang, and Enhong Chen. “*Understanding the Planning of LAG Agents: A Survey.*” *arXiv* (2024)

as small as a general software update.¹⁶ This is to suggest that AI hallucinations are not intending to spread misinformation maliciously, but are a byproduct of combining a labyrinth of data to match its training module into a single task the user gives it. This distinction is what makes hallucinations so dangerous, because popular AI models are programmed to give users the best experience when using the software, and so will generate outputs with the utmost confidence, even if that output is wrong.

In many cases, AI goes beyond and does generate false information intentionally to the user by creating its own pyramid of priorities, often sacrificing truth for other designs, like the overall user experience. An author in *Science* magazine shared an example their friend experienced while interacting with a popular AI model called Claude:

A few weeks ago, a colleague of mine needed to collect and format some data from a website, and he asked the latest version of Anthropic’s generative AI system, Claude, for help. Claude cheerfully agreed to perform the task, generated a computer program to download the data, and handed over perfectly formatted results. The only problem? My colleague immediately noticed that the data Claude delivered was entirely fabricated.

When asked why it had made up the data, the chatbot apologized profusely, noting that the website in question didn’t provide the requested data, so instead the chatbot generated “fictional participant data” with “fake names...and results,” admitting “I should never present fabricated data as if it were scraped from actual sources.”¹⁷

¹⁶ Anqi Shao, “*Beyond Misinformation: A Conceptual Framework for Studying AI Hallucinations in (Science) Communication*,” *arXiv*, April 2025

¹⁷ Melanie Mitchell, “*Why AI Chatbots Lie to Us*,” *Science* 389, no. 6758 (July 24, 2025)

Along the same lines of misaligned priorities in models, is a byproduct that can occur called the “accuracy paradox.”¹⁸ Even when models place a larger emphasis on generating accurate outputs, this does not guarantee reliability, or necessarily reduce the harm it may cause society. One study on the impact of using AI to generate medical discharge instructions for patients found that 18% of the cases had potentially harmful safety issues that were linked to the AI model.¹⁹

Popular AI models such as ChatGPT and Claude have also arguably triggered the most backlash from the general working public, as these versions of AI models often bring about a very sharp love-hate dynamic. For example, customer service jobs report a strong increase in customer resolution statistics from utilizing AI agents (14% increased resolution on average, and 35% for newer workers)²⁰ but they often bring industry wide layoffs and job losses in the same sector. Large scale social and economic disruption, such as the AI takeover of the workforce, can often create instability, which extremist groups have also historically exploited for recruitment.

Terrorist Gen AI Adoption

In addition, there is now an ever-increasing pool of academic research discussing how terrorist groups can use similar models to produce and distribute

¹⁸ Zihao Li, Weiwei Yi, and Jiahong Chen. “Accuracy Paradox: Addressing Epistemic, Manipulative, and Societal Risks of Hallucination in AI Governance.” *Computer Law & Security Review* 58 (2026): 106111

¹⁹ Kristian Stanceski, Sharleen Zhong, Xumou Zhang, Sam Khadra, Marguerite Tracy, Linda Korla, Sarita Lo, Vasi Naganathan, Jinman Kim, Adam G. Dunn, and Julie Ayre, “The Quality and Safety of Using Generative AI to Produce Patient-Centred Discharge Instructions,” *npj Digital Medicine* 7 (2024): 329

²⁰ Erik Brynjolfsson, Danielle Li, and Lindsey R. Raymond. “Generative AI at Work.” *NBER Working Paper* No. 31161. Cambridge, MA: National Bureau of Economic Research, April 2023. Revised November 2023.

false propaganda, often with the end goal of influencing public opinion and policy outcomes. One such example occurred in 2021, when “several reports showed that the unsuspecting Kenyan public was being assaulted with a barrage of AI-generated deepfakes portraying videos of politicians making incendiary statements.”²¹ in preparation for the general election being held in 2022.

Although research indicates that government organizations are already using various models of AI to try and combat extremist groups, a much greater gap exists in how terrorist groups are using that same technology to identify online behaviors that indict who might be a susceptible victim to none-state actors recruitment tactics. However, one common method utilized by terrorist groups and scammers for many decades now is something known as sextortion, or the usage of sexual conversations and images that are meant to be private and then leveraged as blackmail. Gen AI specifically has brought a new fear to many individuals worldwide and that is an emerging form of blackmail known as “deepfake sextortion”, or the creating of false images in the specific likeness of someone and then used as blackmail.²²

AI-generated text-to-image technology, deepfake photo and video manipulation, voice and video generation, and other forms of content manipulation are used to target and exploit children and adults, including for human trafficking, with women and girls disproportionately impacted by crimes like sextortion and child sexual abuse material (CSAM) production (with more than 20,000 AI-generated CSAM images discovered on a single dark web forum in 2024).

²¹ Jake Okechukwu Effoduh. “*The Role and Potential of Artificial Intelligence in Extremist Fuelled Election Misinformation in Africa.*” *Global Network on Extremism & Technology (GNET)*, March 8, 2024

²² U.S. Department of State, *2025 Trafficking in Persons Report* (Washington, D.C.: U.S. Department of State, September 29, 2025)

Unlike a typical large machine learning model that requires millions or billions of tokens of data, terrorists' groups can theoretically create "mini-personalized machine learning models" from smaller sets of stored data tokens to facilitate creating a list of potential individuals who display similar online activity/characteristics as previous victims. Even with small amounts of data, terrorist groups can launch misinformation campaigns targeted towards their desired demographic. One example is when Al-Qaida used the Covid-19 global pandemic to spread their agenda that Covid-19 was "God's wrath on the West."²³

Despite the clear overlap in their functions and applications, the three main forms of AI models remain distinct in how they operate. The easiest way to remember is that machine learning collects, gen AI creates, and AI agents act. A visualization of these three models is presented as Figure One in the Appendix.

Entities and groups operating in illegal spheres face a unique challenge: risks with outsourcing sensitive work. Many corporations who use MLM technology will openly purchase tokenized data or outsource their creation requests to various third parties that already possess the skills and experience to operate the model. However, because outsourcing poses serious risk-mitigation challenges for many non-state actors, the task of using artificial intelligence may eventually be driven to the creation and use of all three models into a singular software/product. There is little research to support the claim

²³ United Nations Interregional Crime and Justice Research Institute and United Nations Counter-Terrorism Centre, *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes*, Turin: UNICRI and UNCCT, 2021)

that terrorist groups have developed a “full tri-operational model” of AI just yet, but supporting evidence may suggest they certainly show a desire to utilize AI, especially generative AI, with examples including ISIS having already developed “how to use AI” manuals and videos in Arabic languages for members of their groups.²⁴

Artificial intelligence has bled into many forms of online media especially social media, often through a pattern known as “the algorithm” or algorithm amplification. To put it plainly, much of the online content a user sees is driven to them based on historical watch history and specific keywords they have used when exploring online. From a business standpoint, corporations believe that when a user sees things they historically engage with, the more time they will theoretically spend on their platform. Customized algorithms can help advertisers target more accurate demographics for their products but can also create issues through something originally dubbed “filter bubbles”²⁵ by Eli Pariser, who says that the internet only promotes ideas to users that they already agree with, and subsequently massively increase instances of confirmation bias.²⁶ Therefore, nonstate actors and terrorist groups can also minimize risk and increase recruitment metrics by customizing messages and online content to be targeted towards users who historically watch and engage with similar content that has led to successful recruitment attempts in the past.

²⁴ Clarisa Nelu. “*Exploitation of Generative AI by Terrorist Groups.*” International Centre for Counter-Terrorism (ICCT), June 10, 2024

²⁵ E. Pariser. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

²⁶ E. Pariser. (2011)

Uneven Research

Overall, the existing literature shows terrorist groups and extremist nonstate actors are adopting artificial intelligence for recruitment and propaganda purposes, specifically generative AI and MLM models. Currently research is still uneven, with most focusing on larger global trends, not specific to Africa or African localized terrorist groups, such as Ahlu Sunnah wa-Jama'a in Mozambique or Boko Haram in Nigeria. In addition, most of the current research details hypothetical or theoretical ways terrorist groups might use AI based on historical analysis, not on how they are currently adopting it. This intelligence gap widens when researching outside of normal AI models used (like Generative AI and AI agents) and into more complex artificial intelligence, such as artificial intelligence drone software (unmanned aerial systems, or UAS) used for surveillance and/or suicide bombings, or facial recognition AI software designed to locate certain individuals or targets.

As a result, important gaps need to be analyzed on how specific African terrorist groups have utilized artificial intelligence, including (but not limited to) the mainstream models of AI, but also complex and less popular forms of AI such as unmanned aerial systems. In this paper, we will seek to fill some of that gap by reviewing one specific case study, which details the terrorist attacks that begin in Mozambique in 2017 following the discovery of natural gas deposits in their northern state, Cabo Delgado, and how artificial intelligence has played a role, and continues to play a role.

Chapter III.

Case Study

This case study examines Mozambique and Ahlu Sunnah wa-Jama'a, focusing on the ongoing terrorist attacks in the northern state of Mozambique, Cabo Delgado, which has led to the displacement of over one million refugees since war began over 425 billion cubic meters of gas that was found offshore in 2010, and analyzes the impact of AI and its facilitation with human trafficking. It will begin by examining the historical context of corruption in Mozambique which led to terrorist attacks in 2017, followed by the humanitarian crisis which has led to the trafficking of thousands of Mozambicans. In conclusion, we will discuss the role of AI in the unfolding of these events and analyze research gaps that need to be addressed for further information.

Origins and Identity of Ahlu Sunnah wa-Jama'a

Cabo Delgado, one of 10 states of the eastern African country Mozambique, is home to the three largest African natural gas projects on the continent. These projects began when Mozambique struck gold in 2010, when a U.S. energy company by the name Anadarko found 425 billion cubic meters of natural gas located just a few miles off the coast of Cabo Delgado.²⁷ The project of extracting the LNG is estimated to produce a new 43 million barrels each year in production for Mozambique. It was not long, however, until various parties outside of the Mozambican government expressed their

²⁷ Al Jazeera. 2020. "Gas-Rich Mozambique May Be Headed for a Disaster." February 24, 2020

interest in the natural gas reservoir and news of the discovered resource quickly spread globally. In 2017, terrorist attacks began in Cabo Delgado by a group dubbed Ahlu Sunnah wa-Jama'a (ASWJ). The group has since pledged its alliance to the Islamic State, and is known by several names such as Ahlu Sunnah wa-Jama'a for its ideology, but also al-Shabaab for its grotesque violence.²⁸ Somalia's leading terrorist group, also known as Al-Shabaab, is believed to have their origins date back to 2006, before pledging its allegiance to Al-Qaeda and later growing to possess somewhere between 7000-12,000 active members.²⁹ However, the "Al-Shabaab" that occupies Mozambique is referred to as Al-Shabaab by the local Mozambicans, while the terrorist group itself claims the name "Ahlu Sunnah Wa-Jamâ" (often abbreviated to Al-Sunnah).³⁰ It is important to note that although they share the same name to many of the Mozambican people as the Somali extremist group, they are considered separate and unconnected from each other. A few years following the initial attacks, they adopted a new name as The Islamic State of Mozambique as well. To avoid potential confusion, in this paper we will refer to the group as Ahlu Sunnah Wa-Jamâ.

The Mozambican extremist group is rather small when compared to the Somali group, and contains somewhere between 300-1000 active members. Much speculation has circled regarding the timeline of the birth of the Mozambican terrorist group, and although a definite origin is unclear, the first reported attacks in 2017 point to Ahlu Sunnah Wa-Jamâ.³¹ Additional theories among locals have circulated around the origins

²⁸ ACLED. "Islamic State Mozambique (ISM)." ACLED, October 30, 2023.

²⁹ National Counterterrorism Center. n.d. "Al-Shabaab (Harakat al-Shabaab al-Mujahideen)."

³⁰ Peter Fabricius, "Is Another Boko Haram or al-Shabaab Erupting in Mozambique?" ISS Today, June 14, 2018, Institute for Security Studies (Pretoria).

³¹ Aslak Orre and Salvador Forquilha, *Poorly Designed Youth Employment Programmes Will Boost the Insurgency in Mozambique*, CMI Brief 2023:2 (Bergen: Chr. Michelsen Institute, 2023)

of the new group which rose to power quickly after the opposition party, RENAMO, signed a peace treaty to end of the civil war in 2014 between RENAMO and FRELIMO (the ruling party since 1975), but most of these rumors are unverified and unsupported.³²

Various aspects of Ahlu Sunnah Wa-Jamâ'a, operations certainly generate curiosity, and unlike a traditional extremist group they do not claim credit for their attacks or even seem to make their motives clear.³³ Although Ahlu Sunnah Wa-Jamâ also rejects the ruling party of FRELIMO, it is important to note it appears to be for different reasons than RENAMO's resistance, so the crossover from a different group is less likely regardless of the strange timeline of events.³⁴

Algorithmic Amplification

Strong evidence supports that the birth of Ahlu Sunnah Wa-Jamâ'a was kickstarted, or at least heavily influenced, by a man named Aboud Rogo Muhammed (1968-2022) who was known for leading the group Al-Hijra in Kenya that previously held ties with al-Qaeda.³⁵ During an interview with an unnamed citizen from Pemba, the capital of Mozambique, they said in regard to Aboud Rogo Muhammed:

I used to listen to him on YouTube; as did many people. He was saying that the government does not help us. If a boss that works for the government commits a crime, nothing happens to him; but if an ordinary Muslim causes a slight

³² Joseph Olusegun Adebayo, "South Africa's Military Deployment to Northern Mozambique: Lessons from the United States of America's (Mis)Adventure in Afghanistan," *Scientia Militaria* 51, no. 1 (2023): 25–43

³³ Joseph Olusegun Adebayo, pg. 26

³⁴ Peter Fabricius. 2018. "Is Another Boko Haram or al-Shabaab Erupting in Mozambique?" *ISS Today*, June 14, 2018.

³⁵ Liazzat J. K. Bonate, "The Jihadi Insurgency in Cabo Delgado: Ideology, Protagonists and Causes." *Kronos* 50, no. 1 (2024).

trouble, the government kills him. The government is corrupt to the core.³⁶

It is important to note that Aboud Rogo Muhammed potentially held a strong audience in Cabo Delgado due to accelerated media algorithms, with his outreach increased due to algorithmic amplification on YouTube. Unlike a lot of social media sites that protect how their algorithms operate under the guise of “trade secrets and security”, YouTube has publicly stated how their recommendation system constantly evolves from billions of data signals daily. The site claims that “to provide such custom curation, our recommendation system doesn’t operate off of a “recipe book” of what to do. It’s constantly evolving, learning every day from over 80 billion pieces of information we call signals.”³⁷ With the level of data that YouTube filters, it contains one of the largest machine learning AI data models in the world.

Extremist content is often controversial, and controversy tends to fare better on overall online engagement scales, but YouTube is an interesting case when examining extremist content where Aboud Rogo Muhammed seemed to grow in popularity. According to a research paper published and funded by the Global Research Network on Terrorism and Technology in 2020, three separate reports suggest that extremist content on YouTube offers a “radicalization pipeline” through displaying similar content through its recommendation algorithm.³⁸ However, the same report mentions a study that “actively discourages users from visiting extreme content.” via YouTube’s

³⁶ Liazzat J. K. Bonate, no. 1. Reference 66

³⁷ YouTube Official Blog. “*On YouTube’s Recommendation System.*” *YouTube Official Blog*, September 15, 2023

³⁸ Joe Whittaker, Seán Looney, Alastair Reed, and Fabio Votta. “*Recommender Systems and the Amplification of Extremist Content.*” *Internet Policy Review* 10, no. 2 (2021): 1–29

recommendation pages, leaving the research mixed.³⁹ Therefore, it is possible that YouTube's algorithmic recommendation system helped spread Aboud Rogo Muhammed's videos and cannot be ruled out as a contributing factor.

Spillover, Displacement and AI-Enabled Translation

Several reported members of the insurgent group include immigrants from other African countries where prominent forms of extremism already existed, and it's possible the newly found group in Mozambique drew in members as a spillover effect, bringing Islamic extremist beliefs from Kenya, and specifically Tanzania, who saw Tanzanian insurgent women join the cause.⁴⁰ Unlike the Al-Shabaab in Somalia, who has sworn a direct allegiance to Al-Qaeda⁴¹, Ahlu Sunnah Wa-Jamâ'a of Mozambique became an affiliate of the Islamic State's Central Africa Province, after a video surfaced of them swearing allegiance to Abu Bakr al-Baghdadi in 2019⁴² and adopting the new name the Islamic State of Mozambique (ISM).

Following the initial attacks in Cabo Delgado in 2017, there have been over 4000 lives lost and a million individuals uprooted from their homes and state.⁴³ (see figure three for a full of displacement numbers.) The attacks have garnered a lot of international attention, such as from UN High Commissioner for Human Rights, Michelle Bachelet, calling for international intervention in Mozambique in relation to the number of human

³⁹ Joe Whittaker, Seán Looney, Alastair Reed, and Fabio Votta no. 2 (2021): 1–29

⁴⁰ Liazzat J. K. Bonate, no. 1. Reference 111

⁴¹ Rasna Warah, "A Legitimate Challenger? Assessing the Rivalry between al-Shabaab and the Islamic State in Somalia," *Combating Terrorism Center at West Point*, June 22, 2020

⁴² Liazzat J. K. Bonate, Paolo Israel, and Carmeliza Rosario, "God, Grievance and Greed: War in Cabo Delgado, Mozambique," *Kronos* 50 (2024)

⁴³ Zenaida Machado, "Five Years On, Justice Still a Dream for Cabo Delgado Victims." Human Rights Watch, November 24, 2022.

rights violations occurring from insurgents.⁴⁴ Many of the crimes being committed include violence, killings, rape, forced marriage and child recruitment, all which go against international humanitarian law.

Large levels of displacement often generate environments that facilitate extreme forms of criminal activity, such as human trafficking and kidnapping, and with the expansion of AI has brought a new dimension more unique to Africa by reducing language barriers through instantaneous algorithmic translations. Africa is home to an estimated 3000 languages, which is roughly 1/3 of all the languages spoken around the globe.⁴⁵ When compared to European Union's 24 officially recognized languages, it is shocking that Mozambique alone contains around 41 languages and dialects.⁴⁶ (refer to figure four for a full list of dialects in Mozambique). According to the OSCE Officer of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings:

AI has enabled traffickers to communicate more fluently in a wider range of languages, including less commonly spoken ones. Previously, the lack of widespread knowledge of these languages had somewhat protected certain linguistic communities from online trafficking recruitment. Now, with AI-powered translation and language generation, these barriers are diminishing.⁴⁷

⁴⁴ Emily Beeken. "UN Rights Chief Calls for Protection of Mozambique Civilians amid Escalating Conflict." JURIST, November 2020.

⁴⁵ UNESCO. "UNESCO and the Promotion of Languages in Africa: Cultural Diversity and Multilingualism." Accessed April 4, 2026.

⁴⁶ Ethnologue, "Mozambique Languages, Literacy, and Maps (MZ)," accessed April 4, 2026.

⁴⁷ Organization for Security and Co-operation in Europe Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, and Regional Support Office of the Bali Process, *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons* (Vienna and Bangkok, 2024).

The language barrier issue is exacerbated even further because of displacement, especially among the elderly, women and children, as being forced from their homes and into a new state or city often means the inability to speak with the new locals which can greatly hinder the integration into a new society. These language barriers heavily impact finding work, which further increases the likelihood of joining an extremist group or becoming a victim to human trafficking. During an interview with an IDP (internally displaced person) from Mozambique they stated: “The fewer people you know, the lower your chances of getting work.”⁴⁸ Some women report the displacement has forced them into undesirable sex work due to overpopulated areas and lack of other work alternatives, with one woman stating: “If I’m lucky, a man will look at me and say they want me for 100 meticaís (\$1.50).”⁴⁹ Reports have spread that various of the local men in Cabo Delgado were given the opportunity to join the new Islamic terrorist group, or be killed, with some estimates placing over 52 men killed in the village Xitaxi, located in the Muidumbe district, after they refused to join against their will.⁵⁰ The convergence of linguistic exclusion and social isolation creates conditions that allow IDP’s to become more vulnerable to coercion and exploitation, where AI language translation from terrorist groups may further reduce pre-existing barriers for recruitment.

⁴⁸ Caitlin Sturridge, João Feijó, and Nelson Tivane, *Coping with the Risks of Conflict, Climate and Internal Displacement in Northern Mozambique: “We Can’t Just Sit Here with Our Arms Crossed”*, HPG Case Study (London: ODI, November 2022) pg. 26

⁴⁹ Caitlin Sturridge, João Feijó, and Nelson Tivane, *Coping with the Risks of Conflict, Climate and Internal Displacement in Northern Mozambique: “We Can’t Just Sit Here with Our Arms Crossed”*, HPG Case Study (London: ODI, November 2022) pg. 33

⁵⁰ Reuters. 2020. “Islamist Insurgents Kill 52 Villagers in Mozambique—Police.” April 22, 2020

Geopolitical Pressure

Despite the growing military threats for the local Mozambicans, international pressure has grown to expedite the newly found gas project in large part due to the war between Russia and Ukraine, and now more recently, the war being the United States and Iran. Since the invasion by President Putin and his forces in the early months of 2022, many countries have condemned Russia's actions and sought to isolate it internationally through a mixture of shown solidarity to Ukraine and a displeasure of the invasion. One such activist, a former Russian chess grandmaster by the name of Gary Kasparov, has ridiculed the European Union for refusing to cut all gas ties and pipelines in and out of Russia.⁵¹ Europe has since attempted to discover various options that do not require relying on Russia's pipelines for their energy needs, and this has brought hope to Total Mozambique's (the company with the largest stake holding in the Cabo Delgado gas project) manager, Maxime Rabilloud. "If it is the aim to stave off Europe from Russian gas, then all LNG gas will be necessary, and that means the project in northern Mozambique, which is massive."⁵² In addition, only several days ago following Iran's decision to "close" the Strait of Hormuz to the United States and their allies, it is estimated that up to 1/5th of the world's oil consumption and 1/5th of the global supply of LNG may be cut off for an indefinite period of time⁵³, which may place even more pressure on Mozambique. TotalEnergies officially restarted their LNG project in January of this year, with the first LNG project expected to finish no sooner than January 2029.⁵⁴

⁵¹ Garry Kasparov. 2015. *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*. PublicAffairs.

⁵² BBC News. 2022. "Mozambique Palma Terror Attack: 'I Can't Go Back.'" March 27, 2022.

⁵³ Mike Fulwood, *Closing the Strait of Hormuz: Impact on the Global Gas Market*, OIES Energy Comment (Oxford: Oxford Institute for Energy Studies, June 2025)

⁵⁴ TotalEnergies, "Mozambique LNG Announces the Full Restart of All Its Activities Onshore and Offshore in Mozambique," January 29, 2026

Corruption in LNG Project Development

Political corruption has been at the forefront of the contested geographical issues in northern Mozambique, with a significant number of issues stemming from individual political and government officers, as well as from soldiers on the ground directly involved in combat. In 2015, the finance minister for Mozambique, Manuel Cheng, was arrested in connection to what has been dubbed “the biggest corruption case in Africa”.⁵⁵ Mozambique, which was currently under governance by the FRELIMO party, had been granted \$2 billion in loans to increase their maritime security and activities, only for several international groups to discover they had been covering up lying about a \$1.4 billion debt (that had been guaranteed by the state) which resulted in the IMF freezing the loans for a six year period.⁵⁶ It was shortly following the implementation of the freeze that Al-Sunnah attacked northern cities of Mozambique, including attacks which eventually overtook the entire city of Pemba and left over 180 Mozambicans trapped within a hotel.⁵⁷

The corruption scandal left many international organizations and countries hesitant to provide any aid to Mozambique as the humanitarian crisis in Cabo Delgado slowly unfolded and displaced so many civilians. In 2022, organizations like the IMF, slowly began to provide assistance, albeit with a much more limited capacity. The IMF granted Mozambique a line of credit worth up to \$456 million (less than 25% of their

⁵⁵ Anonymous GIS Expert. 2023. “*Mozambique Corruption Scandal*.” GIS Reports Online.

⁵⁶ Edson Cortez et al., *Costs and Consequences of the Hidden Debt Scandal of Mozambique* (Maputo, Mozambique / Bergen, Norway: Centro de Integridade Pública [CIP] and Chr. Michelsen Institute, May 2021)

⁵⁷ Al Jazeera News: 2021. “*Over 180 People Trapped in Mozambique Hotel after Attack*.” March 27, 2021.

original \$2 billion amount) with the World bank giving \$300 million.⁵⁸ Many Mozambican citizens were not satisfied at how FRELIMO handled the terrorist attacks in Cabo Delgado (not to mention the embarrassment of being the party responsible for Africa's largest scandal) so many citizens looked to change the country's future at the polls. However, widespread reporting indicated election interference in favor of FRELIMO during the Oct. 2023, local elections, which included various illegal acts, such as voter intimidation and ballot stuffing, and resulted in protests and eventually the deaths of two citizens and injuries to many more.⁵⁹

Mozambique, which still stands as one of the poorest countries in the world, is not currently susceptible to planned online propaganda campaigns that often surface during election times in the same manner that many other countries encounter, since reports show that Mozambique has less than 10% of the overall population with social media accounts⁶⁰, and with only 23.2% of Mozambicans using internet in any manner.⁶¹ Although there is not specific data to determine exactly which demographic of the population those social media users fall, the country follows similar global trends with younger people and urban residents representing a large portion of the users, with urban/non-rural users making up 78.5% of all of internet activity.⁶² Despite lower numbers of online users and even lower social media accounts, Mozambique still encountered a reported 74 fake social media accounts that were designed to spread

⁵⁸ Rédaction Africanews with AFP. "World Bank Gives \$300m Grant to Mozambique after Scandal." Africanews, August 23, 2022.

⁵⁹ Todd Gould. 2023. "2 Dead in Mozambique Protests over Local Election Results, Watchdog Says. Police Say 70 Arrested." AP News, October 27, 2023

⁶⁰ DataReportal. "Digital 2024: Mozambique." *DataReportal*, 2024

⁶¹ DataReportal. "Digital 2024: Mozambique." *DataReportal*, 2024

⁶² Dércio Tsandzana, "Political Parties and Social Media: Between Screenshots, Memes and Hashtags during Municipal Elections in Mozambique," in *Digital Technologies, Elections and Campaigns in Africa*, ed. Duncan Omanga, Admire Mare, and Pamela Mainye (Abingdon, Oxon: Routledge, 2024) pg. 79

misinformation online.⁶³ Although there is no direct evidence that those 74 accounts were AI chatbots or AI created, the example highlights that even small ecosystems of online users can fall victim to online propaganda campaigns, and as AI tools increasingly become cheaper and lower required expertise to use efficiently, Mozambique will most likely see AI generative content swarm its online spaces.

Intelligence Failures

Several surrounding countries have gotten involved in the terrorist issue due to ongoing concerns of potential “spillover effect” from the attacks. Rwanda, another country with history and ties to the Russian Wagner group, deployed 1,000 soldiers to help curb the uprising attacks and humanitarian violations in Cabo Delgado. However, secrecy has shrouded the intentions behind their aid to Mozambique, as the President of Rwanda, Paul Kagame, seemingly deployed the troops without first seeking permission from the Rwandan parliament.⁶⁴ These concerns are further compounded by the broader implications that will arise to the people of Cabo Delgado as a consequence of increased intervention. TotalEnergies, the largest company behind the LNG project in Cabo Delgado, is facing backlash after having criminal charges brought against them for complicity in war crimes that were committed by the Joint Task Force of Mozambique, with a specific instance known as the “container massacre” as its main complaint.⁶⁵

⁶³ European Union Election Observation Mission. *Mozambique 2024 Final Report: General and Provincial Assembly Elections, 9 October 2024*. Brussels: European Union Election Observation Mission, 2024.

⁶⁴ Jason Smith. 2022. “*Rwanda: A Force for Good in Mozambique’s ‘War on Terror’?*” African Arguments, February 9, 2022.

⁶⁵ European Center for Constitutional and Human Rights. “*TotalEnergies Faces Criminal Complaint for Complicity in War Crimes, Torture and Enforced Disappearance in Mozambique.*” ECCHR, November 18, 2025.

The villagers had been caught in the crossfire between the Mozambican army and ISIS-affiliated militants. Having fled their homes, they had gone to seek the protection of government soldiers. Instead, they found horror. The soldiers accused the villagers of being members of the insurgency.

They separated the men — a group of between 180 and 250 — from the women and children. Then they crammed their prisoners into the shipping containers on either side of the entrance, hitting, kicking and striking them with rifle butts.

The soldiers held the men in the containers for three months. They beat, suffocated, starved, tortured and finally killed their detainees. Ultimately, only 26 prisoners survived.⁶⁶

High intense conflict events such as the “container massacre” of Cabo Delgado illustrate both the heightened benefits and serious dangers that can result from artificial intelligence use. On one hand, conflict analysis benefits strongly from AI software due to the model(s) ability to process large quantities of data in a short period of time, particularly satellite imagery. Likewise, AI can also distort public understanding with misinformation developed by generative AI, such as when the internet became so flooded with generative AI of the Hamas attack on Israel, that it left so many individuals doubting even verified evidence, fearing that it might also be AI.⁶⁷ In the case of Cabo Delgado, the tension is striking, as drone use to gather images appears to have evolved more so on the side of the insurgents, and not the side of the state, creating an unique asymmetrical power dynamic. According to Mozambique’s Interior Minister, Amade Miquidade, terrorists wearing the uniforms of the FADM (Armed Forces for the Defense of

⁶⁶ Alex Perry, “In Summer 2021, Mozambican Soldiers Based at a TotalEnergies Gas Plant Abducted, Raped and Killed Dozens of Civilians,” *Politico Europe*, September 26, 2024,

⁶⁷ Cade Metz, “A.I. Muddies Israel-Hamas War in Unexpected Way,” *New York Times*, October 28, 2023

Mozambique) used drones to identify targets, while also using local civilians as human shields.⁶⁸ The asymmetry in intelligence gathering is not surprising considering the issues the Mozambican government has encountered on their home front, especially from their ally, Rwanda. According to Borges Nhamirre, a researcher for the Transnational Threats and Organised Crime, he states that:

Rwandan forces prefer to act unilaterally rather than coordinate with Mozambique's military and police. Mozambique complains that Rwanda doesn't share intelligence and operational information, often taking unilateral decisions. SAMIM sources have shared similar concerns about Rwanda. These sources also say that Mozambique has failed to actively lead the coordination effort as the host country.⁶⁹

While the usage of drones by Ahlu Sunnah wa-Jama'a to identify targets is verified, the existence of AI software connected to these drones is not. It should be noted that determining which drones are AI-enabled can be rather difficult in practice, since onlookers can usually only assess flight patterns, and that alone is not enough to claim artificial intelligence. Even advanced automation and autopilot features do not guarantee the usage of AI software. To establish the existence of artificial intelligence often requires forensic analysis of the software itself, usually from the recovery of the physical drone and examining its hardware.

Tanzania and South Africa both expressed concerns that if the terrorist groups and attacks were not managed, spillover effects could further destabilize the entire region. In

⁶⁸ Crispin Adriaanse, "Using Drones and Disguises, Terrorists Target Northern Mozambique," *IOL*, May 29, 2020

⁶⁹ Borges Nhamirre, "*Cabo Delgado: Two Years since the Palma Invasion*," *Institute for Security Studies*, April 3, 2023

2021, South Africa deployed troops in hopes to reduce the attacks,⁷⁰ despite issues beginning much sooner. In October of 2020, Ahlu Sunnah wa-Jama'a performed several attacks in Mtwara Province in southern Tanzania. The coordinated attacks in the region seemed to be more opportunistic with the upcoming election in Tanzania, than strategic based.⁷¹ The exception seems to be when one gunman killed three police officers and a security guard in 2021 who had been using his social media accounts to follow and access certain Ahlu Sunnah wa-Jama'a's material online.⁷²

Generative AI in African Contexts

According to Shai Farber, "terrorist groups are increasingly deploying AI-powered chatbots and generative models to create false narratives, simulate credible sources, and erode trust in state institutions."⁷³ By contrast, the political unrest following the 2020 elections of Tanzania and later in 2023 and 2024 in Mozambique does not appear to be heavily impacted from generative artificial intelligence, but rather more so influenced by algorithmic recommendation systems that amplify controversial and emotionally charged videos, which allow them to go viral quickly. Following the 2024 general presidential election, reports indicated that the Mozambican government deliberately disrupted internet access

⁷⁰ Joseph Olusegun Adebayo. "South Africa's Military Deployment to Northern Mozambique: Lessons from the United States of America's (Mis)Adventure in Afghanistan." *Scientia Militaria* 51, no. 1 (2023): 25–43.

⁷¹ Judd Devermont, and Marielle Harris. n.d. "Making Sense of the Hype: What We Know about ISIS-Mozambique's Attacks in Tanzania." *Fraym Blog*.

⁷² Nick Dausen. "Tanzania Says Gunman Who Killed Four People Last Month Was a Terrorist." *Reuters*, September 2, 2021

⁷³ Shai Farber. "AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security." *Journal of Strategic Security* 18, no. 3 (2025): 320–44

in response to large scale protests and viral online content that emerged from announced presidential results.⁷⁴

In the lead up to South Africa's general election in 2024, notable instances of AI created videos circulated on WhatsApp. Some memorable examples that approached viral levels of engagement included deepfake videos that falsely depicted President Joe Biden issuing a warning that if the African National Congress (ANC) were to win the election, the United States would pose heavy sanctions, as well as a video of the popular rapper Eminem falsely vocally supporting the Economic Freedom Fighters.⁷⁵ So although the Mozambican political climate does not appear to be driven by the same level of generative AI as South Africa, Mozambique is seeing a rapid exponential increase in internet usage over the last decade, which will make them increasingly vulnerable to AI-assisted misinformation campaigns in the near future.

To put into perspective, Mozambique saw internet users increase by 842,000 users just from January 2023-January 2024, which was an increase of 11.8% from the previous year.⁷⁶ At the same time, these figures should be interpreted with caution, since fewer than 24% of Mozambicans currently have internet access, meaning overall connectivity to online spaces remains mostly limited, despite the exponential growth.

Election cycles present attractive opportunities for cyber-attacks and online manipulation by extremist groups because they combine three main characteristics:

⁷⁴ Daniela Pulido, "Mozambique Restricts Social Media Access Amid Post-Election Protests and Rights Concerns," *JURIST*, November 2, 2024

⁷⁵ Gregory Gondwe, "AI-Driven Disinformation and Political Influence on WhatsApp in South Africa's 2024 Elections," *The International Journal of Press/Politics* (November 2025): 1–20

⁷⁶ DataReportal. "Digital 2024: Mozambique." *DataReportal*, 2024

Compressed time frames that hinder thorough factchecking, large online reach, and controversial algorithmic amplification. As mentioned earlier, election cycles are particularly vulnerable to AI generated propaganda campaigns because they often unfold in quick time frames that restrict the ability to fact-check effectively. In addition, generative AI has made the process of creating more “deceptive” propaganda campaigns easier than ever before, and much more accessible. Detecting misinformation online is a hurdle, that often requires multiple steps and a lengthy timeframe, which are several characteristics that social media does not prioritize or encourage from its creators. According to Jiexun Li and Xiaohui Chang, combating the spread of online misinformation requires not only the detection of false or misleading content, but a more accessible fact-checking solution than what current exists on social media platforms.⁷⁷

Unlike other forms of scientific research that often require years of study and approval before being shared with the general population, social media creates an environment where any post containing false information can go viral within moments. Since many sites grant anonymity to their creators through the creation of usernames, terrorist groups have been known to utilize social media to help facilitate the spreading of false propaganda. One such example is from a study completed in 2021, where researchers examined how social media bots were used by the Islamic state on a social site called Telegram:

The 106 bots we identified via Telegram’s API were either active in or mentioned on ninety-eight distinct groups and thirty-seven distinct channels. Their level of activity was significant: collectively, they posted some 39,211 messages. Most of these were published in groups (33,487 in groups and 5,724 in channels). . . On average, the bots posted 176

⁷⁷ Jiexun Li and Xiaohui Chang, “Combating Misinformation by Sharing the Truth: A Study on the Spread of Fact-Checks on Social Media,” *Information Systems Frontiers* 25, no. 4 (2023): 1479–1493

messages each day (140 text, thirteen images, twelve PDFs, four video clips, and two audio files).⁷⁸

In the case of Mozambique, although a majority of citizens lack access to social media accounts or direct internet access, mobile devices as a way of communication still exists as a primary form of communication. “Of all the countries surveyed, Mozambique has the lowest mobile phone adoption level and the second highest gender disparity at 36 percent after Rwanda’s 38 percent. More than half of all men (50%) have mobile phones as compared to only 32 percent of women. The disparities are more pronounced among Internet users.”⁷⁹ (see figure four.)

The Role of WhatsApp

Emphasizing the level of internet consumption is important because many Mozambicans rely more heavily on sites such as WhatsApp, than on traditional social media sites due to the free access of texting and calling that the app provides. It is also worth noting that many reports and academic studies do not label WhatsApp and Telegram as standard forms of social media but instead are sometimes grouped separately as “private messaging platforms”. This distinction raises concerns that some literature on social media use in Africa may be analytically limited,⁸⁰ since platforms such as WhatsApp are among the most widely used digital communications tools when discussing African contexts,

⁷⁸ A. Alrhoun, Winter, C., & Kertész, J. (2024). *Automating Terror: The Role and Impact of Telegram Bots in the Islamic State’s Online Ecosystem*. *Terrorism and Political Violence*, 36(4), 409–424

⁷⁹ Alison Gillwald, Onkokame Mothobi, and Broc Rademan, *The State of ICT in Mozambique 2018*, RIA Policy Paper no. 6, vol. 5, After Access (Cape Town: Research ICT Africa, January 2019)

⁸⁰ DataReportal. “Digital 2024: Mozambique.” *DataReportal*, 2024. Accessed April 5, 2026.

while still containing similar characteristics of standard social media. WhatsApp has enormous global reach, approximately 2.3 billion monthly users⁸¹, which exceeds that of even Facebook's 2.25 billion monthly users⁸², and therefore also suffers from a vulnerability to misuse and the spread of AI generated misinformation.

Apps like WhatsApp allow for end-to-end encryption, which is very appealing in an age where user privacy is held to a high regard, especially when other popular sites like Telegram do not offer the same encryption protection (there are some exceptions, such as Telegram's "secret chats" feature).⁸³ However, it subsequently generates an environment that is less risky for interactions between extremist recruiters and their potential recruits. WhatsApp allows for one-on-one interactions between parties without the risk of data being tracked (from even the hosting company itself) whereas Telegram channels offer unlimited subscribers, which brings a greater capacity for large-scale dissemination.

At their cores, WhatsApp theoretically allows for personal interactions by extremists, and Telegram theoretically allows for faster distribution of misinformation. In terms of AI chatbots, WhatsApp requires a business API license code to operate a bot, whereas Telegram offers an open bot API for users⁸⁴, further signaling Telegram's potential to spread misinformation quickly.

⁸¹ Simon Kemp, "Digital 2024 October Global Statshot Report," *DataReportal*, October 23, 2024

⁸² Simon Kemp, "Digital 2024 October Global Statshot Report," *DataReportal*, October 23, 2024

⁸³ Dilip Kumar Patairya, "Telegram vs. WhatsApp — The Encryption War," *Cointelegraph*, August 29, 2024

⁸⁴ Dilip Kumar Patairya, "Telegram vs. WhatsApp — The Encryption War," *Cointelegraph*, August 29, 2024

However, WhatsApp and Telegram data are not reported into social media statistics for Mozambique⁸⁵ so understanding their full role and relations to insurgent groups is very limited.

Overall, Mozambique's case study demonstrates that AI technology is evolving, but still extremely limited in cases like overall internet consumption. While more research needs to be conducted on how terrorist groups in Mozambique use WhatsApp for propaganda distribution and whether AI generative misinformation is already being dispersed, the pattern is clear: even in limited digital environments, various advanced forms of technology are already being deployed by Ahlu Sunnah wa-Jama'a, such as the use of drones for targeted strikes and reconnaissance, while state institutions continue to struggle to coordinate comparable technologies and achieve the regional cooperation necessary to restore lasting peace in Cabo Delgado.

⁸⁵ DataReportal. "Digital 2024: Mozambique." *DataReportal*, 2024. Accessed April 5, 2026.

Chapter IV:

Analysis and Discussion

The Mozambican case study of Cabo Delgado provides an important basis for analyzing how emerging artificial intelligence interacts with terrorist adaption from African conflicts. Although direct evidence of sophisticated artificial intelligence usage is limited in some areas, the study reveals that extremist groups can still exploit available communications systems in Southern Africa (such as WhatsApp) and utilize more advanced technological innovations like drones and generative AI during presidential election cycles to achieve their goals. This chapter discusses the broader implications of these findings with an emphasis on five key areas: uneven technological adoption, evidentiary and attribution problems, asymmetrical power dynamics, public policy implications, future risks and jailbreaking, and finally the broader implications for Africa.

Uneven Technological Adoption

To begin, the conflict in Cabo Delgado is shaped by an asymmetrical power structure in which civilians receive the least amount of protection yet embrace the largest consequences from both insurgent violence and the local police abuse. While AI can be beneficial when it can facilitate conflict monitoring, such as when it was used as a predictive model that accurately predicted over 98% of attacks⁸⁶, it can also greatly inflict

⁸⁶ Ume Kalsooma, Sahar Arshad, Amerah Albarah, Imran Siddiqi, Saeed Ullah, Abdul Mateen, and Farhan Amin. “*A Big Data Driven Multilevel Deep Learning Framework for Predicting Terrorist Attacks.*”

damage, such as generative AI deepfakes that spread like wildfire through WhatsApp during the South African Presidential general elections in 2024.⁸⁷

Extremist groups do not need to achieve full technological parity with the latest software available to gain a meaningful advantage. In African conflict zones, even the selective adoption of basic technology, like over the counter drones, is sufficient to magnify existing weaknesses in governance that arises from nonexistent intelligence coordination between neighboring countries and/or intense political fragmentation from contested elections. The Mozambican case in particular shows that even when internet access and overall digital consumption is limited and extremely low nationwide, terrorist organizations like Ahlu Sunnah wa-Jama'a are still able to adjust and incorporate operational technology like drones into conflict zones to gain an advantage. Although there are reports that the Mozambican police force is beginning to use drones as well⁸⁸, it is striking that publicly reported insurgent drones use appears more visible than documented state drone use, despite the government's €285 million allocated for its defense budget.⁸⁹

The question then becomes how does a government that spends a quarter of a billion dollars on national security yearly, appear to lag so far behind the insurgent attacks? Even when dispersing technological resources, the state military appears to be sluggish in doing so, only offering some cities and villages small advances at a time, such as when they offered Nampula only two drones to increase surveillance⁹⁰ with a promise

⁸⁷ Gregory Gondwe, "AI-Driven Disinformation and Political Influence on WhatsApp in South Africa's 2024 Elections," *The International Journal of Press/Politics* (November 2025): 1–20

⁸⁸ Mozambique: *Nampula Government Offers Two Drones to Boost Surveillance*, Club of Mozambique, December 1, 2025

⁸⁹ Club of Mozambique: *Mozambique to Cut Direct Defence Budget by 35% in 2025*, May 8, 2025

⁹⁰ Mozambique: *Nampula Government Offers Two Drones to Boost Surveillance*, Club of Mozambique, December 1, 2025

of eight more in the future (which in politically divided ecosystems, would not be surprising if they were unable to fulfill.)

Evidentiary and Attribution Problems

At the same time, the Mozambique case highlights the evidentiary limitations that are lacking from research on artificial intelligence in Africa. Some examples include a possible misalignment of definitions, seeing how some of the current literature does not include WhatsApp usage reports in their surveys, despite having more monthly users than Facebook and many similar features to other forms of social media.⁹¹ Although there is existing literature which groups WhatsApp into social media categories when considering African online consumption, some sources do not include it in the final tallies.⁹² However, it is more likely that for the case of Mozambique in particular, that the lack of WhatsApp user data stems from there simply being no data to collect surrounding the app's usage in the country at all, not from an active decision to exclude it when discussing social media applications.⁹³

Research regarding mobile app use in Mozambique has struggled historically to form definitive conclusions, with mobile data indicators showing no data to report prior to 2015⁹⁴ with additional complications arising from families sharing mobile devices across members. While pinpointing demographic trends and their connection to online behavior may pose a difficult challenge on their own, self-censorship may also alter digital

⁹¹ Simon Kemp, “*Digital 2024 October Global Statshot Report*,” *DataReportal*, October 23, 2024

⁹² DataReportal. “Digital 2024: Mozambique.” *DataReportal*, 2024. Accessed April 5, 2026.

⁹³ DataReportal. “Digital 2024: Mozambique.” *DataReportal*, 2024. Accessed April 5, 2026.

⁹⁴ Marcelino Tayob. *ICT Data Collection: International Best Practices and Lessons Learned*. Presented at the A4AI-Mozambique Expert Workshops, Maputo, Mozambique, July 7, 2015. International Telecommunication Union, 2015. Pg. 33

behavior arising from awareness that a user's online actions may potentially be observed by other family members. A report published in 2025⁹⁵ regarding female phone surveys in Mozambique, showed several issues complicated ensuring privacy among participants. Some respondents answered, stating:

It's very difficult, he has to come back so I can borrow his phone... now, I'm the one who usually recharges it... yes, yes, yes. Yes, when I want to talk to people far away I have to wait for him to get back from work to call me so I can talk." (004-Mobile phone interviewee)

I can't answer where others are listening. Yes, I would answer differently. (0002-mobile phone interviewee)

I can answer with reservations because there are things that I can't answer when I'm with someone else. (00010-in-person interviewee)⁹⁶

Therefore, much more research needs to be done regarding mobile phone usage in Mozambique to help understand how insurgent groups are utilizing generative AI and other artificial intelligence technology to disrupt social systems.

Another example is that while drone deployment (UAS) may be noticeable to onlookers, determining whether such systems are AI-enabled requires forensic and technical evidence that is rarely available in conflict zones that are still highly active since it would require recovering the physical drone itself. A similar issue arises with separating fake accounts made to spread misinformation online. Although there are many

⁹⁵ Rosemary Morgan, Yolanda Manganhe, Celso Monjane, Milly Nakatabira, Helen Kuo, Cremildo Manhiça, Ferão Mandlate, Milton Sengo, Midalia Uamba, Almamy Malick Kante, Ivalda Macicame, and Agbessi Amouzou. "Women's Participation in Mobile Phone Surveys in Mozambique: Findings from a Qualitative Study." *Tropical Medicine & International Health* 30, no. 9 (September 2025): 946–953

⁹⁶ Morgan et al., "Women's Participation in Mobile Phone Surveys in Mozambique," 946-953

indicators of AI-assisted technology during online use (such as coordinated messaging or instantaneous response times) they are often difficult to confirm conclusively since it would require the same level of forensic investigation and technical evidence gathering as referenced with UAS technology.

Asymmetrical Power Dynamics

Asymmetry does not simply mean that there is one weaker and one stronger party in a conflict. Power during terrorists' conflicts is never a basic scoreboard where tallies are always black, white, or definitive in nature. State governments possess material power like large defense budgets, but insurgents possess disruptive power, such as fear and psychological pressure. The asymmetry is further swayed when considering corruptive governments and tense political environments. In the case of Mozambique, the presence of Ahlu Sunnah wa-Jama'a in Cabo Delgado refers to the unbalanced approach that grants each side of the conflict specific strengths and weaknesses. For example, the smaller size of ASWJ allowed them to disperse and adopt their strategies with more ease following the intervention from Rwanda, to avoid losing total control in the region.⁹⁷ Despite having a large defense budget, ASWJ has been able to displace over a million individuals and turn upside the economy of Mozambique. However, the corruptive nature of the Mozambican government allowed for coordinated media blackouts following the national elections on a national scale.⁹⁸

⁹⁷ Institute for Security Studies, "Are Rwandan Troops Becoming Cabo Delgado's Main Security Provider?" *ISS Today*, 2024

⁹⁸ Daniela Pulido, "Mozambique Restricts Social Media Access Amid Post-Election Protests and Rights Concerns," *JURIST*, November 2, 2024

In the case of AI, even small amounts of generative AI images can heavily impact social trust online and impact information pipelines. Without proper AI protection legislation in place, various uses of artificial intelligence technology like language translators to reduce tribal communication barriers can greatly benefit insurgent groups when attempting to commit crimes, such as human trafficking.⁹⁹

Public Policy Implications

From a public policy perspective, these findings suggest that the challenge is not preventing the newest and most advanced forms of artificial intelligence from being abused but rather responding to uneven and asymmetrical forms of technical adaptation that arises from governing gaps. Governments should seek how emerging technology interacts with their specific vulnerabilities in conflict environments in order to form adequate protection for civilians and military personnel. For example, Mozambique should seek to strengthen cross-border intelligence with neighboring countries, such as Rwanda¹⁰⁰, and expand research into how communication platforms such as WhatsApp and Telegram are used by insurgent groups. They should also seek to develop artificial intelligence legislation that not only offers greater protection to its users, but additional internet privacy layers that include more rights towards individuals when shared mobile devices exist within families.¹⁰¹

⁹⁹ Organization for Security and Co-operation in Europe Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, and Regional Support Office of the Bali Process, *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons* (Vienna and Bangkok, 2024)

¹⁰⁰ Nhamirre Borges, “Cabo Delgado: Two Years since the Palma Invasion,” *Institute for Security Studies*, April 3, 2023

¹⁰¹ Rosemary Morgan, Yolanda Manganhe, Celso Monjane, Milly Nakatabira, Helen Kuo, Cremildo Manhiça, Ferão Mandlate, Milton Sengo, Midalia Uamba, Almamy Malick Kante, Ivalda Macicame, and

Future Risks and Jailbreaking

Although there is limited evidence of terrorist groups in Africa systematically deploying fully jailbroken AI models, the concern remains relevant. Jailbroken models not only circumvent programmed safeguards, but may also lead to a larger asymmetry through something I call malicious model piggybacking (or MMP). MMP describes a situation when a jailbroken model can not only be used to generate prohibited outputs, but also helps infer restrictions and detection patterns imposed on the standard versions of the same model. From this standpoint, the jailbroken model now becomes a tutor for malicious actors that can teach them how systems are regulated, and where normal detection and prevention limits are programmed. In simpler terms, it is making the AI model your double agent, who snitches on itself to you. Therefore, jailbreaking puts companies and governments that are obligated to follow the original safeguards at a disadvantage compared to any malicious actor who manages to jailbreak the AI model(s).

Malicious model piggybacking can specifically impact the financial world through the modern adaptation of crypto currencies by facilitating the ability to automate deceptive messaging and obscure transactions patterns through the acceleration of funds across various accounts. It also gives malicious users an understanding of how normal detection methods function, therefore offering alternative methods for users to conceal and launder money more efficiently on blockchains.

Agbessi Amouzou. "Women's Participation in Mobile Phone Surveys in Mozambique: Findings from a Qualitative Study." *Tropical Medicine & International Health* 30, no. 9 (September 2025): 946–953

Although some government agencies may receive specialized access to AI systems through tailored partnerships (such as OpenAI for government program)¹⁰² countries like the U.S. are still required to operate within the bounds of existing legal and regulatory frameworks, such as FISMA. Violent nonstate actors and insurgent groups, however, are not usually held back by such restrictions, which may allow them to exploit jailbroken and manipulated systems that further widen the gap to create more asymmetry between state and nonstate actors. In the case of Mozambique and Africa, many countries do not possess any legislation regarding AI, or at the very least the inability to enforce it effectively.

Broader Implications for Africa

When considering the broader implications of the impact of Mozambique, two things need particular focus: the spillover effects and different AI applications by other countries. Mozambique as a case study paints a different picture than various other countries in Africa since it currently sits as the 9th poorest country in the world by GDP per capita at only \$656.80 per person.¹⁰³ As mentioned before, South Africa has been introduced to generative AI interference during their political elections, after several examples of prominent community figures going viral for speaking about some candidates.¹⁰⁴ Tanzania is already suffering from spillover effects due to ISIS-Mozambique, with two large attacks occurring in the Michenjele and Kitaya villages,

¹⁰² OpenAI. “*Introducing OpenAI for Government.*” OpenAI, June 16, 2025.

¹⁰³ World Bank, “*GDP per Capita (Current US\$),*” *World Development Indicators*, accessed April 13, 2026

¹⁰⁴ Gregory Gondwe, “*AI-Driven Disinformation and Political Influence on WhatsApp in South Africa’s 2024 Elections,*” *The International Journal of Press/Politics* (November 2025): 1–20

both in the Mtwara Region, which borders Mozambique.¹⁰⁵ Rwandan deployments have helped quell the conflicts surrounding the LNG project zones, but in a limited capacity as the insurgents seemly were propelled outwards to other areas, not removed.¹⁰⁶

The bilateral agreement to deploy Rwandan troops in Mozambique was, and remains, secret. It is known only to the two countries' top leadership and was never submitted to the Mozambique Parliament. This led to [contestation](#), especially by Mozambique's defence and security sector watchdogs such as the parliamentary opposition, the media and civil society organisations...

They have reduced the insurgents' firepower, dislodged them from their main bases, and restored stability around the LNG projects. Yet their capacity and inclination for hot pursuit have displaced the problem, with terror groups dispersing and regrouping in other locations.¹⁰⁷

Without knowing the full reason for Rwanda's intervention, compiled with the apparent lack of intelligence sharing between both countries, further complicates efforts to assess regional impact.

¹⁰⁵ U.S. Department of State, *Country Reports on Terrorism 2020: Tanzania* (Washington, DC: U.S. Department of State, 2020)

¹⁰⁶ Institute for Security Studies, "Are Rwandan Troops Becoming Cabo Delgado's Main Security Provider?" *ISS Today*, 2024

¹⁰⁷ Institute for Security Studies, "Are Rwandan Troops Becoming Cabo Delgado's Main Security Provider?" *ISS Today*, 2024

Chapter V.

Conclusion

Artificial intelligence is growing and evolving at a rate that is unprecedented in humankind. African conflict zones suffer from uneven and selective technology use, but not always the most highly sophisticated. Even in extreme limited digital spaces like Mozambique, where less than 24% of citizens have access to the internet¹⁰⁸ insurgent groups can adapt and take advantage of government gaps from institutional conflict. Asymmetry between state and nonstate actors AI use is important to analyze because currently some insurgent groups can exploit faster than a government can respond.

Intelligence sharing between African nations suffers from political tension and high corruption and in some cases, can be nonexistent between neighboring countries. Artificial intelligence technology is growing and evolving faster than the rate of adoption by Africans who live without mobile devices. Generative AI poses one of the largest threats during political elections, due to algorithmic amplification of controversial material. Therefore, the challenge is not simply a question of how much technology is accessible, but how much coordination, governance (or lack of) and speed exists when using that technology.

The central lesson is that AI will not affect African conflicts in a uniform way, but when institutional weakness arrives from poor intelligence sharing and highly charged political environments, it can sharpen the advantages for disruptive non-state actors. As AI technology becomes cheaper, faster and more accessible, the gap between

¹⁰⁸ DataReportal. “Digital 2024: Mozambique.” *DataReportal*, 2024

technological opportunity and state responses may evolve into one of the most important security challenges in all of Africa.

Appendix.

Figures and Maps

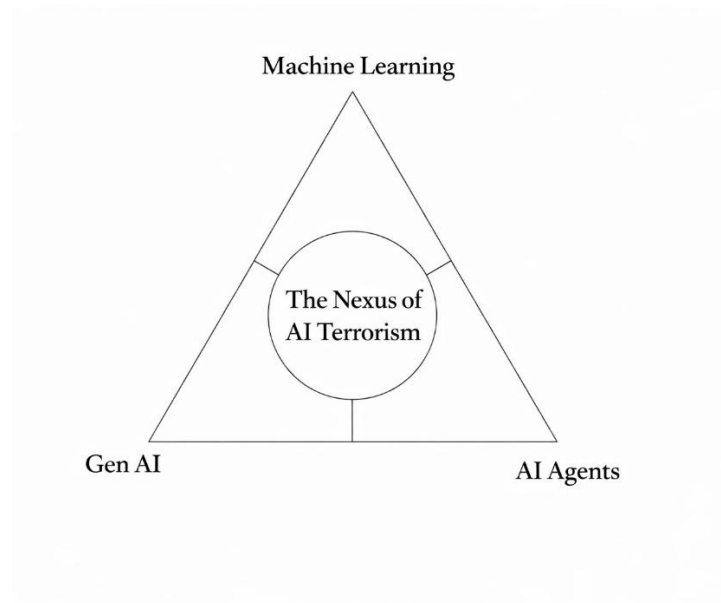


Figure 1 .The Nexus of AI Terrorism¹⁰⁹

Source: Author's own work, created with OpenAI's Gen AI

¹⁰⁹ Huffaker, Ethan. 2026. *The Nexus of AI Terrorism*. Original figure created by the author with assistance from OpenAI generative AI tools.

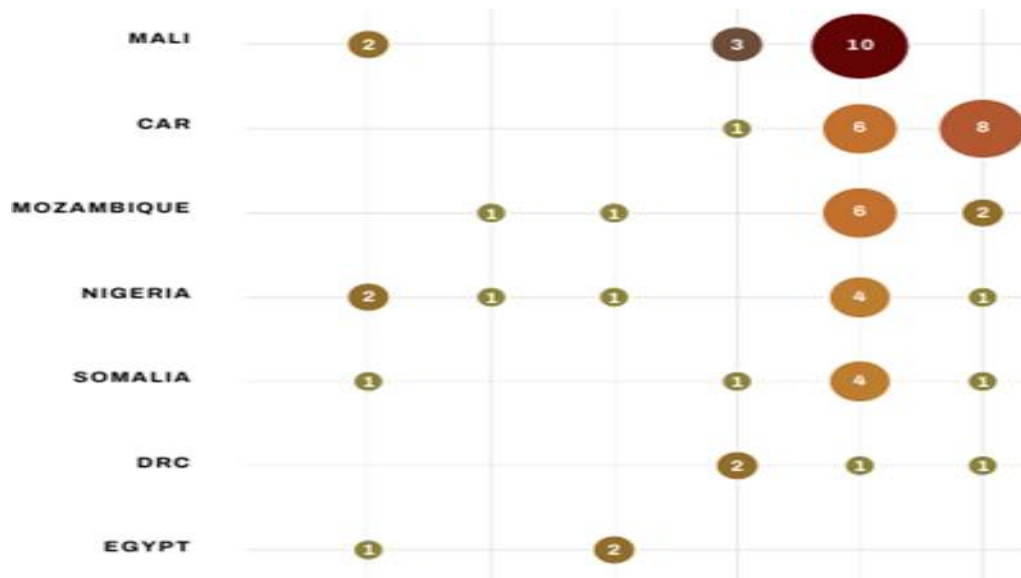


Figure 2. Recorded Incidents of UASs' Use by NSAGs in Africa

Source: Moraes Figueiredo, Bárbara. "The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa."

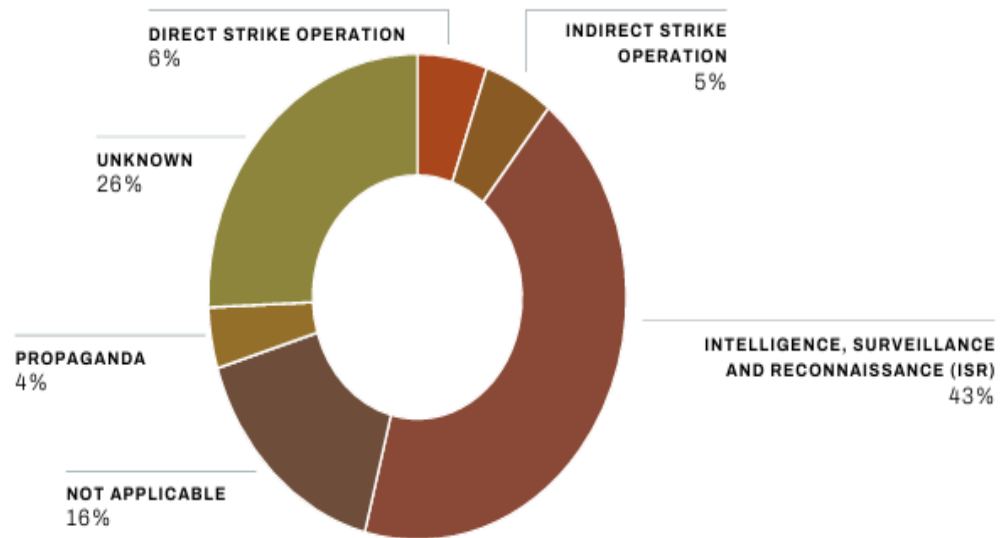


Figure 3. Types of Use of UAS by NSAGs in Africa, January 2018–June 2023

Source: Morais Figueiredo, Bárbara. “The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa

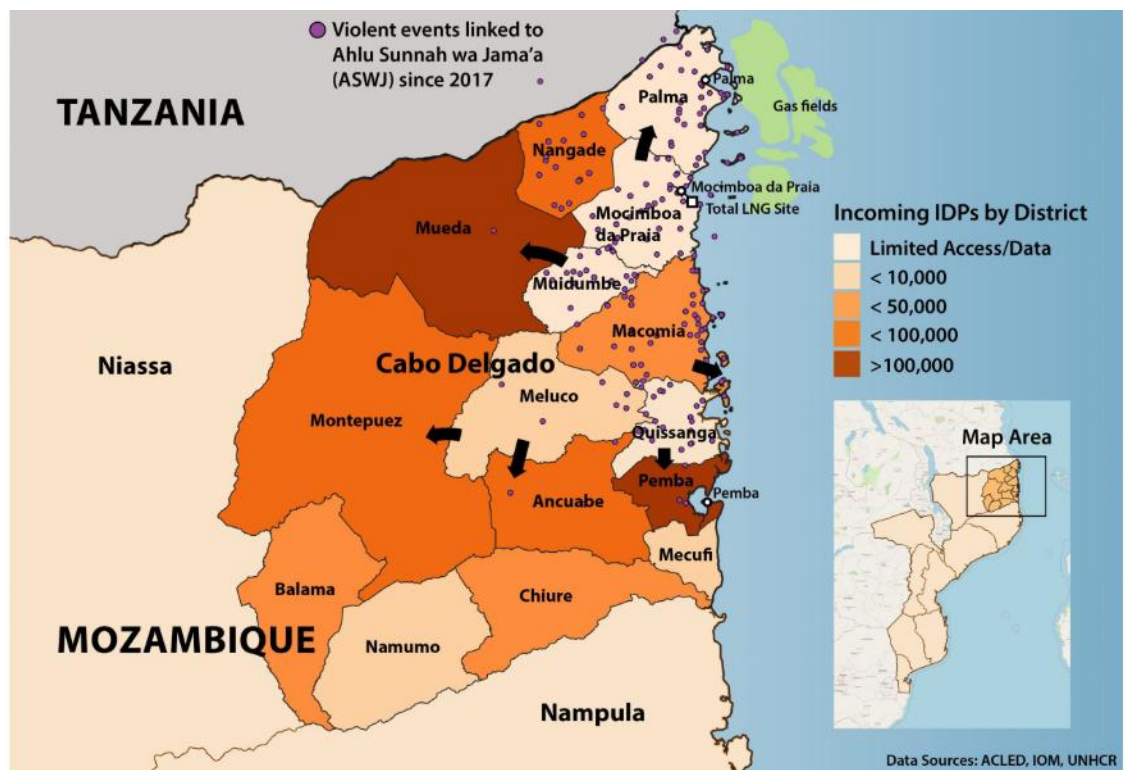


Figure 4. Map of Displacements in Cabo Delgado

Source: Africa Center for Strategic Studies. "Cries from the Community: Listening to the People of Cabo Delgado." Africa Center for Strategic Studies, 2021

bwg Barwe	xmc Makhuwa-Marrevone	wmw Mwani	twl Tawara
ccc Chopi	mgh Makhuwa-Meetto	ndc Ndau	twx Tewe
chw Chuwabu	mhm Makhuwa-Moniga	nse Nsenga	toh Tonga
dmx Dema	xsq Makhuwa-Saka	nya Nyanja	tso Tsonga
kzn Kokola	vmk Makhuwa-Shirima	nyu Nyungwe	tsc Tswa
eko Koti	kde Makonde	phm Phimbi	xmq Xingoni
kdn Kunda	ymk Makwe	mg Ronga	yao Yao
lib Lolo	mny Manyawa	seh Sena	zul Zulu
ngl Lomwe	mxk Manyika	swl Swahili	
cwb Maindo	vmr Marenje	ssw Swati	
vmw Makhuwa	mzy Mozambican Sign Language	tkw Takwane	

Figure 5. List of Indigenous Languages Spoken in Mozambique

Source: *Ethnologue*, “Mozambique Languages, Literacy, and Maps (MZ

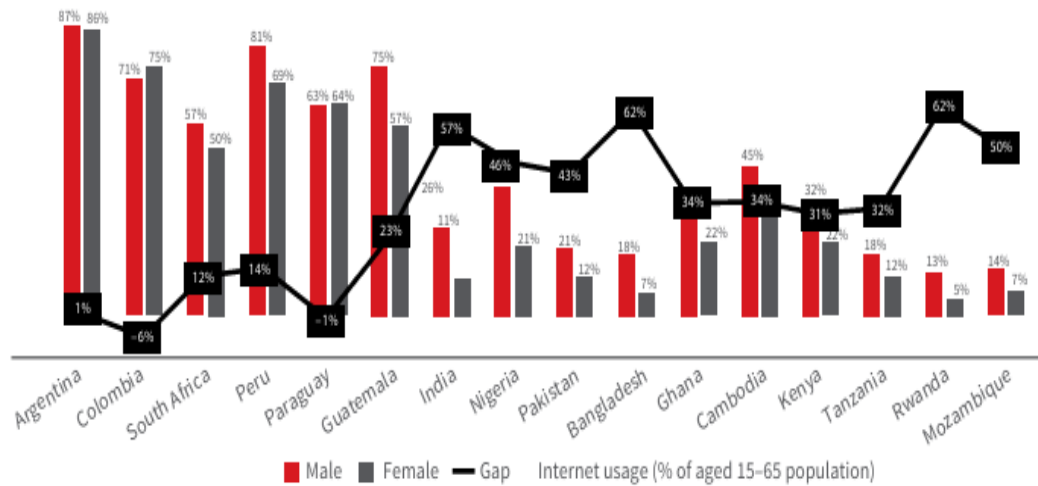


Figure 6. Gender Disparity in Internet Use, Mozambique & Other African Countries.

Source: Alison Gillwald, Onkokame Mothobi, and Kudzai Ratan, *The State of ICT in Mozambique 2018* (Cape Town: Research ICT Africa, 2019), fig. 7

References

ABC News. n.d. “*Mueller: Suicide Bomber Recruited in U.S. FBI Director: Naturalized U.S. Citizen Carried Out Suicide Bombing in Somalia.*” Accessed September 5, 2025. <https://abcnews.go.com/TheLaw/Terrorism/story?id=6942162>.

ACLED. “Islamic State Mozambique (ISM).” *ACLED*, October 30, 2023 [Islamic State Mozambique \(ISM\) | ACLED](#)

ACN International. 2023. “Mozambique: Terrorists Kill 11 Christians in Attack in the Province of Cabo Delgado.” September 21, 2023. <https://acninternational.org/mozambique-terrorists-kill-11-christians-in-attack-in-the-province-of-cabo-delgado/>.

Adebayo, Joseph Olusegun. “South Africa’s Military Deployment to Northern Mozambique: Lessons from the United States of America’s (Mis)Adventure in Afghanistan.” *Scientia Militaria* 51, no. 1 (2023): 25–43. <https://doi.org/10.5787/51-1-140>

Adriaanse, Crispin. “Using Drones and Disguises, Terrorists Target Northern Mozambique.” *IOL*, May 29, 2020. <https://iol.co.za/news/africa/2020-05-29-using-drones-and-disguises-terrorists-target-northern-mozambique/>.

Al Jazeera. 2020. “Gas-Rich Mozambique May Be Headed for a Disaster.” February 24, 2020. <https://www.aljazeera.com/opinions/2020/2/24/gas-rich-mozambique-may-be-headed-for-a-disaster#:~:text=When%2C%20in%202010%2C%20US%20energy,gas%20field%20in%20the%20area>.

Al Jazeera News: 2021. “Over 180 People Trapped in Mozambique Hotel after Attack.” March 27, 2021. <https://www.bing.com/videos/riverview/relatedvideo?q=over-180-people-trapped-in-mozambique-hotel-after-isil-attack.&mid=5FC4C7D3CDC60B61B0415FC4C7D3CDC60B61B041&FORM=VIRE>

Alrhoun, A., Winter, C., & Kertész, J. (2024). Automating Terror: The Role and Impact of Telegram Bots in the Islamic State’s Online Ecosystem. *Terrorism and Political Violence*, 36(4), 409–424, <https://doi.org/10.1080/09546553.2023.2169141>

Amnesty International. 2019. “Mozambique: Detained Journalist in Critical Condition Denied Medical Treatment.” March 5, 2019. <https://www.amnesty.org/en/latest/news/2019/03/mozambique-detained-journalist-in-critical-condition-denied-medical-treatment/>.

- Amundsen, Inge. 2014. "Drowning in Oil: Angola's Institutions and the 'Resource Curse.'" *Comparative Politics* 46 (2): 169–189.
<http://www.jstor.org/stable/43664097>.
- Anonymous GIS Expert. 2023. "Mozambique Corruption Scandal." GIS Reports Online.
<https://www.gisreportsonline.com/r/mozambique-corruption-scandal/>.
- BBC News. 2022. "Mozambique Palma Terror Attack: 'I Can't Go Back.'" March 27, 2022. <https://www.bbc.com/news/world-africa-61029991>.
- Beeken, Emily. 2020. "UN Rights Chief Calls for Protection of Mozambique Civilians amid Escalating Conflict." JURIST, November 2020.
<https://www.jurist.org/news/2020/11/un-rights-chief-calls-for-protection-of-mozambique-civilians-amid-escalating-conflict/>.
- Bergen, Peter. 2015. "How Big of a Threat Is Al-Shabaab to the United States?" CNN, February 22, 2015. <https://www.cnn.com/2015/02/22/opinion/bergen-al-shabaab-threat/>.
- Bode, Ingvild, and Anna Nadibaidze. "AI and Drones in the Russian Invasion of Ukraine: Challenging the Expectations?" AutoNorms. Accessed March 18, 2026.
<https://www.autonorms.eu/ai-and-drones-in-the-russian-invasion-of-ukraine-challenging-the-expectations/>.
- Bonate, Liazzat J. K. "The Jihadi Insurgency in Cabo Delgado: Ideology, Protagonists and Causes." *Kronos* 50, no. 1 (2024). <https://doi.org/10.17159/2309-9585/2024/v50a11>
- Bonate, Liazzat J. K., Paolo Israel, and Carmeliza Rosario. "God, Grievance and Greed: War in Cabo Delgado, Mozambique." *Kronos* 50 (2024).
<https://doi.org/10.17159/2309-9585/2024/v50a18>.
- Brynjolfsson, Erik, Danielle Li, and Lindsey R. Raymond. "Generative AI at Work." NBER Working Paper No. 31161. Cambridge, MA: National Bureau of Economic Research, April 2023. Revised November 2023.
<https://doi.org/10.3386/w31161>.
- Carnegie Council for Ethics in International Affairs. "Nuclear Deterrence." *Ethics & International Affairs*. Accessed September 5, 2025. Carnegie Council for Ethics in International Affairs, "Nuclear Deterrence," *Ethics & International Affairs*,
- CNN Wire Staff. 2012. "Al-Shabaab Joining al Qaeda, Monitor Group Says." CNN, February 10, 2012. <https://www.cnn.com/2012/02/09/world/africa/somalia-shabaab-qaeda/index.html>.
- Committee to Protect Journalists. 2023. "Mozambican Journalist Leonardo Gimo Investigated for Criminal Defamation over Report on Alleged Police Corruption."

June 27, 2023. <https://cpj.org/2023/06/mozambican-journalist-leonardo-gimo-investigated-for-criminal-defamation-over-report-on-alleged-police-corruption>.

Cortez, Edson, Aslak Orre, Baltazar Fael, Borges Nhamirre, Celeste Banze, Inocência Mapisse, Kim Harnack, and Torun Reite. *Costs and Consequences of the Hidden Debt Scandal of Mozambique*. Maputo, Mozambique / Bergen, Norway: Centro de Integridade Pública (CIP) and Chr. Michelsen Institute, May 2021 4442-Costs-and-consequences-of-the-Hidden-Debt-FINAL.pdf

Cross-Border Cooperation Could Curb Kidnappings in Mozambique. 2023. AllAfrica.com. SyndiGate Media Inc.

Cruz, João de Almeida da. 2022. "Fueling Insurgency: Liquefied Natural Gas, ISIS, and Green Berets in Mozambique." Modern War Institute, March 18, 2022. <https://mwi.westpoint.edu/fueling-insurgency-liquified-natural-gas-isis-and-green-berets-in-mozambique/#:~:text=In%20March%202021%2C%20roughly%20a,train%20the%20Mozambican%20armed%20forces>.

DataReportal. "Digital 2024: Mozambique." DataReportal, 2024. Accessed April 5, 2026. <https://datareportal.com/reports/digital-2024-mozambique>

Dausen, Nick. 2021. "Tanzania Says Gunman Who Killed Four People Last Month Was a Terrorist." Reuters, September 2, 2021. <https://www.reuters.com/world/africa/tanzania-says-gunman-who-killed-four-people-last-month-was-terrorist-2021-09-02/>.

Devermont, Judd, and Marielle Harris. n.d. "Making Sense of the Hype: What We Know about ISIS-Mozambique's Attacks in Tanzania." Fraym Blog. <https://fraym.io/blog/isis-mozambique-tanzania/>.

Dilip Kumar Patairya, "Telegram vs. WhatsApp — The Encryption War," Cointelegraph, August 29, 2024, <https://cointelegraph.com/learn/articles/telegram-vs-whatsapp-encryption-war>

Doherty, Ben. 2017. "Climate Change Will Fuel Terrorism Recruitment, Report for German Foreign Office Says." The Guardian, April 20, 2017. <https://www.theguardian.com/environment/2017/apr/20/climate-change-will-fuel-terrorism-recruitment-adelphi-report-says>.

Ebhuoma, Ebele, Mapira Simatele, Llewellyn Leonard, Ovie Ebhuoma, Francis Donkor, and Henry Tantoh. 2020. "Theorising Indigenous Farmers' Utilisation of Climate Services: Lessons from the Oil-Rich Niger Delta." Sustainability 12 (9): Article 87349. <https://doi.org/10.3390/su12187349>.

Effoduh, Jake Okechukwu. "The Role and Potential of Artificial Intelligence in Extremist Fuelled Election Misinformation in Africa." *Global Network on Extremism &*

Technology (GNET), March 8, 2024 The Role and Potential of Artificial Intelligence in Extremist Fuelled Election Misinformation in Africa – GNET

Ethnologue, “Mozambique Languages, Literacy, and Maps (MZ),” accessed April 4, 2026.

European Union Election Observation Mission. Mozambique 2024 Final Report: General and Provincial Assembly Elections, 9 October 2024. Brussels: European Union Election Observation Mission, 2024.

<https://www.europarl.europa.eu/cmsdata/298609/Mozambique%20-%20General%20Elections%2C%209%20October%202024%2C%20EU%20EOM%20Final%20Report.pdf>

European Center for Constitutional and Human Rights. “TotalEnergies Faces Criminal Complaint for Complicity in War Crimes, Torture and Enforced Disappearance in Mozambique.” ECCHR, November 18, 2025. <https://www.ecchr.eu/en/press-release/totalenergies-faces-criminal-complaint-for-complicity-in-war-crimes-torture-and-enforced-disappearance-in-mozambique/>

Fabricius, Peter. 2018. “Is Another Boko Haram or al-Shabaab Erupting in Mozambique?” ISS Today, June 14, 2018. <https://issafrica.org/iss-today/is-another-boko-haram-or-al-shabaab-erupting-in-mozambique>.

Farber, Shai. “AI-Enabled Terrorism: A Strategic Analysis of Emerging Threats and Countermeasures in Global Security.” *Journal of Strategic Security* 18, no. 3 (2025): 320–44. <https://doi.org/10.5038/1944-0472.18.3.2377>

Fulwood, Mike. Closing the Strait of Hormuz: Impact on the Global Gas Market. OIES Energy Comment. Oxford: Oxford Institute for Energy Studies, June 2025
Comment-Closing-the-Strait-of-Hormuz-impact-on-the-Global-Gas-Market.pdf

2022. “SADC and Rwandan Troops Disperse Mozambique Insurgents — but Displace More Civilians.” *Daily Maverick*.

Ghazvinian, John. 2008. *Untapped: The Scramble for Africa’s Oil*.

Gillwald, Alison, Onkokame Mothobi, and Kudzai Ratan. *The State of ICT in Mozambique 2018*. Cape Town: Research ICT Africa, 2019
<https://researchictafrica.net/wp-content/uploads/2019/07/the-state-of-ict-in-mozambique.pdf>

Gigova, Radina. “Who Vladimir Putin Thinks Will Rule the World.” CNN, September 2, 2017. <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>

Gondwe, Gregory. “AI-Driven Disinformation and Political Influence on WhatsApp in South Africa’s 2024 Elections.” *The International Journal of Press/Politics* (November 2025): 1–20. <https://doi.org/10.1177/19401612251395434>

- Gould, Todd. 2023. "2 Dead in Mozambique Protests over Local Election Results, Watchdog Says. Police Say 70 Arrested." AP News, October 27, 2023. <https://apnews.com/article/mozambique-protests-elections-frelimo-renamo-df8adc444d6b36fa9b03cfff6d772e1>.
- Huang, Xu, Weiwen Liu, Xiaolong Chen, Xingmei Wang, Hao Wang, Defu Lian, Yasheng Wang, Ruiming Tang, and Enhong Chen. "Understanding the Planning of LAG Agents: A Survey." arXiv (2024). [2402.02716] Understanding the planning of LLM agents: A survey
- Huffaker, Ethan P. 2026. The Nexus of AI Terrorism. Original figure created by the author with assistance from OpenAI Generative AI tools.
- Ibrahim, Adam, Benjamin Thérien, Kshitij Gupta, Mats L. Richter, Quentin Anthony, Timothée Lesort, Eugene Belilovsky, and Irina Rish. "Simple and Scalable Strategies to Continually Pre-train Large Language Models." Transactions on Machine Learning Research, June 2024. <https://arxiv.org/pdf/2403.08763>
- Institute for Security Studies. "Are Rwandan Troops Becoming Cabo Delgado's Main Security Provider?" ISS Today, 2024 <https://issafrica.org/iss-today/are-rwandan-troops-becoming-cabo-delgado-s-main-security-provider?>
- Iroanya, Richard O. 2018. Human Trafficking and Security in Southern Africa: The South African and Mozambican Experience. Palgrave Macmillan.
- Iroanya, Richard Obinna. "Policy Responses to Human Trafficking in Mozambique and South Africa." In Human Trafficking and Security in Southern Africa, 185–224. Springer International Publishing AG. https://doi.org/10.1007/978-3-319-71988-7_6.
- Kalsooma, Ume, Sahar Arshad, Amerah Albarah, Imran Siddiqi, Saeed Ullah, Abdul Mateen, and Farhan Amin. "A Big Data Driven Multilevel Deep Learning Framework for Predicting Terrorist Attacks." Scientific Reports 15 (2025): Article 23060. <https://doi.org/10.1038/s41598-025-08201-0>
- Kasparov, Garry. 2015. Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped. PublicAffairs.
- Kemp, Simon. "Digital 2024 October Global Statshot Report." DataReportal. October 23, 2024. <https://datareportal.com/reports/digital-2024-october-global-statshot>
- Li, Jiexun, and Xiaohui Chang. "Combating Misinformation by Sharing the Truth: A Study on the Spread of Fact-Checks on Social Media." Information Systems Frontiers 25, no. 4 (2023): 1479–1493. <https://doi.org/10.1007/s10796-022-10296-z>
- Li, Zihao, Weiwei Yi, and Jiahong Chen. "Accuracy Paradox: Addressing Epistemic, Manipulative, and Societal Risks of Hallucination in AI Governance." Computer

Law & Security Review 58 (2026): 106111.
<https://doi.org/10.1016/j.clsr.2026.106311>

- Loch, Patrick. 2022. "U.S. Government Designates al-Shabaab Financial Facilitators to Thwart Revenue Streams." United States Africa Command, October 21, 2022. <https://www.africom.mil/article/34807/us-government-designates-al-shabaab-financial-facilitators-to-thwart-revenue-streams>.
- Luna, Nandini, Lars Vredenburg, and Inês Pereira. 2023. "What Is the Wagner Group? The 'Brutal' Russian Military Unit in Ukraine. The U.S. Has Labeled Them a 'Criminal Organization.'" ABC News, August 23, 2023. <https://abcnews.go.com/International/International/wagner-group-brutal-russian-military-group-fighting-ukraine/story?id=96665326>.
- Machado, Zenaida. 2022. "Five Years On, Justice Still a Dream for Cabo Delgado Victims." Human Rights Watch, November 24, 2022. <https://www.hrw.org/news/2022/11/24/five-years-justice-still-dream-cabo-delgado-victims>.
- Machado, Zenaida. 2023. "Southern African Leaders Silent over Abuses in Mozambique: Publish Results of Announced Investigation; Provide Redress to Victims." Human Rights Watch, August 18, 2023. <https://www.hrw.org/news/2023/08/18/southern-african-leaders-silent-over-abuses-mozambique>.
- Mitchell, Melanie. "Why AI Chatbots Lie to Us." *Science* 389, no. 6758 (July 24, 2025): eaea3922. <https://doi.org/10.1126/science.aea3922>.
- Metz, Cade. "A.I. Muddies Israel-Hamas War in Unexpected Way." *New York Times*, October 28, 2023. <https://www.nytimes.com/2023/10/28/business/media/ai-muddies-israel-hamas-war-in-unexpected-way.html>
- Mohammed, Kayode. 2021. "A Wealth of Sorrow: Why Nigeria's Abundant Oil Reserves Are Really a Curse." *The Guardian*, November 9, 2021. <https://www.theguardian.com/global-development/2021/nov/09/a-wealth-of-sorrow-why-nigerias-abundant-oil-reserves-are-really-a-curse>.
- Morais Figueiredo, Bárbara. *"The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa."* Geneva: United Nations Institute for Disarmament Research, 2024. <https://doi.org/10.37559/CAAP/24/PACAV/01>
- Morgan, Rosemary, Yolanda Manganhe, Celso Monjane, Milly Nakatabira, Helen Kuo, Cremildo Manhiça, Ferão Mandlate, Milton Sengo, Midalia Uamba, Almamy Malick Kante, Ivalda Macicame, and Agbessi Amouzou. "Women's Participation in Mobile Phone Surveys in Mozambique: Findings from a Qualitative Study." *Tropical Medicine & International Health* 30, no. 9 (September 2025): 946–953. Women's participation in mobile phone surveys in Mozambique: Findings from a qualitative study - Morgan - 2025 - Tropical Medicine & International Health - Wiley Online Library

- Mozambican Journalist Leonardo Gimo Investigated for Criminal Defamation over Report on Alleged Police Corruption. 2023. AllAfrica.com. SyndiGate Media Inc.
- Mozambique: Nampula Government Offers Two Drones to Boost Surveillance,” Club of Mozambique, December 1, 2025
<https://clubofmozambique.com/news/mozambique-nampula-government-offers-two-drones-to-boost-surveillance>
- Mozambique Police Arrest Four State Officials for Corruption. 2017. Agence de Presse Africaine (APAnews). SyndiGate Media Inc.
- Club of Mozambique: Mozambique to Cut Direct Defence Budget by 35% in 2025.”, May 8, 2025 <https://clubofmozambique.com/news/mozambique-to-cut-direct-defence-budget-by-35-in-2025>
- National Counterterrorism Center. n.d. “Al-Shabaab (Harakat al-Shabaab al-Mujahideen).” https://www.dni.gov/nctc/terrorist_groups/al_shabaab.html
- National Counterterrorism Center, Department of Homeland Security, and Federal Bureau of Investigation, *Violent Extremists’ Use of Generative Artificial Intelligence* (Joint Counterterrorism Assessment Team, 2024)
 151s_First_Responders_Toolbox-Violent_Extremists_Use_of_Generative_Artificial_Intelligence.pdf
- Nelu, Clarisa. “Exploitation of Generative AI by Terrorist Groups.” International Centre for Counter-Terrorism (ICCT), June 10, 2024.
<https://icct.nl/publication/exploitation-generative-ai-terrorist-groups>
- News Agencies. 2019. “Mozambique President, Renamo Leader Sign Peace Deal.” Al Jazeera, August 1, 2019. <https://www.aljazeera.com/news/2019/8/1/mozambique-president-renamo-leader-sign-peace-deal>
- Nhamirre, Borges. “Cabo Delgado: Two Years since the Palma Invasion.” Institute for Security Studies, April 3, 2023. <https://issafrica.org/iss-today/cabo-delgado-two-years-since-the-palma-invasion>
- OpenAI. “Introducing OpenAI for Government.” OpenAI, June 16, 2025.
<https://openai.com/global-affairs/introducing-openai-for-government/>
- Organization for Security and Co-operation in Europe Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, and Regional Support Office of the Bali Process. *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons*. Vienna and Bangkok, 2024. Flyer Template
- Orre, Aslak, and Salvador Forquilha. Poorly Designed Youth Employment Programmes Will Boost the Insurgency in Mozambique. CMI Brief 2023:2. Bergen: Chr. Michelsen Institute, 2023. <https://www.cmi.no/publications/8798-poorly->

designed-youth-employment-programmes-will-boost-the-insurgency-in-mozambique

- Pariser, Eli. *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press, 2011.
- Perry, Alex. 2022. "Attack on Amarula Hotel in Palma, Mozambique, Africa." *Outside Online*, May 31, 2022. <https://www.outsideonline.com/outdoor-adventure/exploration-survival/attack-amarula-hotel-palma-mozambique-africa/>
- Perry, Alex. "In Summer 2021, Mozambican Soldiers Based at a TotalEnergies Gas Plant Abducted, Raped and Killed Dozens of Civilians." *Politico Europe*, September 26, 2024. <https://www.politico.eu/article/totalenergies-mozambique-patrick-pouyanne-atrocities-afungi-palma-cabo-delgado-al-shabab-isis/>
- Pulido, Daniela. "Mozambique Restricts Social Media Access Amid Post-Election Protests and Rights Concerns." *JURIST*, November 2, 2024. Mozambique restricts social media access amid post-election protests and rights concerns - JURIST - News
- Quirós-Fons, Alba. 2022. "Religious Persecution in Sub-Saharan Africa: Jihadism and ICC Prosecution." *Religions* 13 (9): 784. <https://doi.org/10.3390/rel13090784>.
- Rabasa, Angel, Peter Chalk, Kimberly Cragin, Sara A. Daly, Heather S. Gregg, Theodore W. Karasik, Kevin A. O'Brien, and William Rosenau. 2006. "Al-Qaeda's Finances." In *Beyond al-Qaeda: Part 1, The Global Jihadist Movement*, 57–62. RAND Corporation. <http://www.jstor.org/stable/10.7249/mg429af.12>.
- Rampe, William. 2023. "What Is Russia's Wagner Group Doing in Africa?" *Council on Foreign Relations*, May 23, 2023. <https://www.cfr.org/in-brief/what-russias-wagner-group-doing-africa>.
- Rédaction Africanews with AFP. 2022. "World Bank Gives \$300m Grant to Mozambique after Scandal." *Africanews*, August 23, 2022. <https://www.africanews.com/2022/08/23/world-bank-gives-300m-grant-to-mozambique-after-scandal/>.
- Reuters. 2020. "Islamist Insurgents Kill 52 Villagers in Mozambique—Police." April 22, 2020. <https://www.reuters.com/article/us-mozambique-insurgency-idUSKCN2233AV>.
- Saltmarsh, Matthew. 2022. "Nearly 1 Million People Have Fled Five Years of Northern Mozambique Violence." *UNHCR*, October 4, 2022. <https://www.unhcr.org/us/news/briefing-notes/nearly-1-million-people-have-fled-five-years-northern-mozambique-violence>.

- Shao, Anqi. “Beyond Misinformation: A Conceptual Framework for Studying AI Hallucinations in (Science) Communication,” arXiv, April 2025
<https://arxiv.org/html/2504.13777v1>
- Smith, Jason. 2022. “Rwanda: A Force for Good in Mozambique’s ‘War on Terror’?” African Arguments, February 9, 2022.
<https://africanarguments.org/2022/02/rwanda-a-force-for-good-in-mozambiques-war-on-terror/>.
- Southern African Development Community. 2022. “Member States.”
<https://www.sadc.int/member-states>.
- Stanceski, Kristian, Sharleen Zhong, Xumou Zhang, Sam Khadra, Marguerite Tracy, Linda Koria, Sarita Lo, Vasi Naganathan, Jinman Kim, Adam G. Dunn, and Julie Ayre. “The Quality and Safety of Using Generative AI to Produce Patient-Centred Discharge Instructions.” npj Digital Medicine 7 (2024): 329.
<https://doi.org/10.1038/s41746-024-01336-w>
- Sturridge, Caitlin, João Feijó, and Nelson Tivane. Coping with the Risks of Conflict, Climate and Internal Displacement in Northern Mozambique: “We Can’t Just Sit Here with Our Arms Crossed”. HPG Case Study. London: ODI, November 2022. Coping with the risks of conflict, climate and displacement in northern Mozambique
- Tayob, Marcelino. ICT Data Collection: International Best Practices and Lessons Learned. Presented at the A4AI-Mozambique Expert Workshops, Maputo, Mozambique, July 7, 2015. International Telecommunication Union, 2015
https://adi.a4ai.org/wp-content/uploads/2015/06/ITU_work_ICT_statistics_A4AI_MPM.pdf
- Tech Against Terrorism. Early Terrorist Experimentation with Generative Artificial Intelligence Services. Briefing, November 2023.
<https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf>
- The Meir Amit Intelligence and Terrorism Information Center. 2023. “Spotlight on Global Jihad (August 9–16, 2023).” <https://www.terrorism-info.org.il/en/spotlight-on-global-jihad-august-9-16-2023/>.
- TotalEnergies. “Mozambique LNG Announces the Full Restart of All Its Activities Onshore and Offshore in Mozambique.” January 29, 2026 [totalenergies_pr-mozambique-LNG-announces-full-restart-all-activities-onshore-and-offshore-in-mozambique_2026_en.pdf](https://www.totalenergies.com/press-releases/2026/01/29/mozambique-lng-announces-full-restart-all-activities-onshore-and-offshore-in-mozambique_2026_en.pdf)
- Tsandzana, Dércio. “Political Parties and Social Media: Between Screenshots, Memes and Hashtags during Municipal Elections in Mozambique.” In Digital

- Technologies, Elections and Campaigns in Africa, edited by Duncan Omanga, Admire Mare, and Pamela Mainye, 75–90. Abingdon, Oxon: Routledge, 2024. <https://doi.org/10.4324/9781003429081-6>.
- Tvedten, Inge, and Rachi Picardo. 2018. “‘Goats Eat Where They Are Tied Up’: Illicit and Habitual Corruption in Mozambique.” *Review of African Political Economy* 45 (158): 541–557. <https://doi.org/10.1080/03056244.2018.1546686>.
- UNESCO. “UNESCO and the Promotion of Languages in Africa: Cultural Diversity and Multilingualism.” Accessed April 4, 2026 UNESCO and the promotion of languages in Africa: cultural diversity
- United Nations Interregional Crime and Justice Research Institute and United Nations Counter-Terrorism Centre, Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes (Turin: UNICRI and UNCCT, 2021), <https://www.un.org/counterterrorism/sites/default/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf>
- U.S. Department of State. 2023. “Mozambique.” 2023 Trafficking in Persons Report. June 15, 2023. <https://www.state.gov/reports/2023-trafficking-in-persons-report/mozambique/>.
- U.S. Department of State, Country Reports on Terrorism 2020: Tanzania (Washington, DC: U.S. Department of State, 2020) <https://www.state.gov/reports/country-reports-on-terrorism-2020/tanzania>
- Vhumbunu, Clayton H. 2020. “Combating Human Trafficking in the Southern African Development Community: Strategies, Challenges, and Opportunities.” *Strategic Review for Southern Africa* 42 (2): 179–203. <https://doi.org/10.35293/srsa.v42i2.7>.
- Warah, Rasna. “A Legitimate Challenger? Assessing the Rivalry between al-Shabaab and the Islamic State in Somalia.” *Combating Terrorism Center at West Point*, June 22, 2020. A Legitimate Challenger? Assessing the Rivalry between al-Shabaab and the Islamic State in Somalia - Combating Terrorism Center at West Point
- Whittaker, Joe, Seán Looney, Alastair Reed, and Fabio Votta. “Recommender Systems and the Amplification of Extremist Content.” *Internet Policy Review* 10, no. 2 (2021): 1–29. <https://doi.org/10.14763/2021.2.1565>
- YouTube Official Blog. “On YouTube’s Recommendation System.” YouTube Official Blog, September 15, 2023 On YouTube’s recommendation system - YouTube Blog
- Zeichick, Alan. “AI vs. GenAI vs. ML: Key Differences.” Oracle, May 9, 2025. <https://www.oracle.com/artificial-intelligence/ai-vs-gen-ai-vs-ml/>