Assessing the Impact of Major Transnational Security Threats in Africa: A Governance and Human Security Perspective

Irene K. Maswan[1], Prof. Sam Nyanchoga[2]

[1]Postgraduate Student, School of Arts and Social Sciences, PhD in Social Transformation, Tangaza University, Kenya

[2]Lecturer, School of Arts and Social Sciences, Tangaza University, Kenya

DOI: https://doi.org/10.68050/JAMS.2026.554

Received: 20 Sept 2026; Accepted: 21 Sept 2026; Published: 22 September 2026

ABSTRACT

Transnational security threats in Africa, such as violent extremism, organized crime, cybercrime and maritime insecurity, are often discussed separately and tackled from a state-centric, military-oriented perspective. The paper is based on Critical Security Studies. Political Economy approaches, with a qualitative documentary analysis of 54 institutional, academic and journalistic sources published between 2020 and 2026, and makes four claims: (1) the four threat domains are not analytically separable; (2) criminal syndicates exploit both digital and maritime infrastructure;

(3) the four exploit the same underlying governance deficits; and (4) the four cannot be coercively contained. To make the convergence claim more specific, the paper identifies five forms of interconnections between threat domains (from the same actors committing multiple crimes to shared infrastructure and enabling conditions to causal linkages) and explicitly excludes mere co-occurrence. It then maps six governance deficits (corruption and institutional capture, weak justice, limited regulatory capacity, border-management gaps, financial opacity, and socio-economic exclusion) onto each domain. It explores the political economy of extremist rebellion, the institutionalization of the illegal market, the increasingly digital surface and its weaponization against civil liberties, and the land-sea connection between illegal, unreported and unregulated (IUU) fishing and piracy. Two empirical cases support this analysis: Burkina Faso, whose number of deaths due to terrorism dropped from 1,907 in 2023 to 1,532 in 2024, and 846 in 2025, without resolving the root causes of the conflict; and the Democratic Republic of Congo (DRC) where approximately 70 per cent of the world's mined cobalt is produced, and 81.1 per cent of the population is living in extreme poverty, with more than 7.3 million people displaced. At the end of 2024, sub-Saharan Africa hosted 38.8 million internally displaced persons. Securitization paradox — increased security by the state, decreased security for the people — requires a move from coercion to governance: a human security approach with financial transparency, accountable justice systems and effective regional cooperation.

Keywords: transnational security; human security; violent extremism; organized crime; cybercrime; maritime insecurity; governance; Africa

INTRODUCTION

In today's Africa, security is increasingly organized, capitalized and realized in a cross-border environment. Armed non-state actors rely on regional supply chains; transnational criminal networks use local brokers to access global illicit markets; cybercriminal networks exploit cross-jurisdictional digital infrastructure; and maritime crime networks integrate onshore logistical corruption with offshore criminal activities. While national institutions are the main pillars of security, there must be multilateral and regional coordination, as no single state can provide comprehensive monitoring, investigation, and prosecution of transnational security networks (Döring, 2023).

This paper examines and critically analyzes four interconnected areas of transnational insecurity: violent extremism, organized crime, cybercrime, and maritime insecurity. While analytically distinct, these threats converge – and convergence isn't a single thing. However, based on the typology presented in the conceptual framework below, the paper identifies five different ways through which threat domains are interconnected: actors that engage in several types of criminality; actors that use the same infrastructure in different ways; enabling conditions that are shared by threat domains; causal links between threat domains; and mere simultaneity—that is, threat domains that occur at the same time, but with no causal relationship between them. The paper's claims are only for the first 4 types. The domains overlap significantly within this qualification, for example, when armed groups use networks for illegal trafficking and smuggling, when criminal syndicates rely on digital tools such as encryption and false documents, and when port corruption and financial laundering are key commodities of maritime crime. The line between criminal armed groups and political actors begins to blur in contexts of poor governance (Idler, 2020; Muggah, 2023).

The paper argues that the norm of securitizing these transnational threats, which are usually defined as state-based, can at times aggravate the governance gaps it is meant to address, as well as the human rights violations which are part and parcel of securitization. Mitigation thus needs to go beyond coercive countermeasures to a comprehensive approach that combines human security, financial transparency and equitable regional governance.

Transnational insecurity has repercussions beyond immediate death and destruction. It systematically undermines human development, raises regional trade costs, and undermines the social contract. By the end of 2024, there were 38.8 million internally displaced persons (IDPs) in sub-Saharan Africa, the highest number in the region and representing 46 percent of the global IDP population (IDMC, 2025), underscoring insecurity as a key structural barrier to sustainable development in the region.

METHODOLOGY

Research Design and Rationale

This study adopts a qualitative, desk-based documentary design. It combines secondary institutional, academic, and journalistic sources to explore Africa's transnational security threats. Given the nature of this topic, a secondary-data approach is analytically appropriate, as primary fieldwork in high-risk areas (e.g., the Central Sahel, eastern Democratic Republic of Congo (DRC), the Gulf of Guinea and Cabo Delgado) is often impossible in the face of acute security concerns, limited humanitarian access, and the logistical and ethical challenges associated with conducting fieldwork in conflict-affected communities. This triangulation across three types of sources, institutional, journalistic, and peer-reviewed, allows the study to create a credible and multi-perspectival picture of dynamics that would not have been possible in a reasonable time period using only one of the three types of sources by a single researcher.

Search Strategy and Documentation Selection

The documents were identified by targeted searches during the period of March–September 2026 in the following public databases: (i) public repositories of the main institutional producers in this field, such as the Institute for Economics and Peace (Global Terrorism Index editions 2024–2026), the UN Office on Drugs and Crime (UNODC), the UN Development Programme (UNDP), the UN Conference on Trade and Development (UNCTAD), INTERPOL, the ICC International Maritime Bureau (IMB), the Internal Displacement Monitoring Centre (IDMC), the Africa Organised Crime Index (ENACT), the World Bank Group, the African Union and ECOWAS, the UN Office for the Coordination of Humanitarian Affairs (OCHA), and the International Organization for Migration's Displacement Tracking Matrix; and (ii) Google Scholar, using the following combination of keywords: each threat domain, plus the regional and thematic focus (e.g., "violent extremism Sahel", "transnational organized crime Africa index", "cybercrime Africa threat assessment", "piracy IUU fishing Gulf of Guinea", "illicit financial flows Africa", "internal displacement Published documents remaining in the collection were used to create foundational and canonical works that preceded 2020 by means of snowball sampling.

The review was confined to English-language sources or official English translations of Francophone and Lusophone institutional documents. The selection process involved four stages. First, 162 documents were identified. Second, 138 duplicates remained for screening after removing 24. Third, titles and abstracts were filtered using the following inclusion/exclusion criteria, which excluded 84 documents based on scope, period, and source. Third, 84 documents were filtered based on the following inclusion/exclusion criteria for titles and abstracts: scope, period, and document sources. Fourth, the remaining 54 documents were evaluated in full text and then included in the synthesis for this study, serving as the works cited. The evidence retained by threat domain, source type, publication year, geographical focus, and principal finding is summarised in Table 1. A search log documenting the queries, date of queries, and disposition of each of the documents that were scanned is available on request from the corresponding author.

Table 1: Summary of documentary evidence by threat domain, source type, year, geographical focus and principal finding

Source (year)	Type	Domain	Geographic focus	Principal finding/evidence used
IEP, Global Terrorism Index (2024; 2025; 2026)	Institutional index	Violent extremism	Global; Sahel	Sahel >50% of 2025 terrorism deaths; global deaths fell 28% to 5,582; five countries (Pakistan, Burkina Faso, Nigeria, Niger, DRC) ≈70% of deaths
Africa Center for Strategic Studies (2025); GI-TOC-2023	Institutional / NGO research	Violent extremism; organized crime	Sahel	JNIM's diversified war economy: gold taxation, kidnapping-for-ransom (×30 in Burkina Faso 2017–2022), coerced zakat, livestock theft
Thurston (2020); Zenn (2020; 2021)	Academic	Violent extremism	Sahel; Lake Chad Basin	Localisation of jihadist ideology in communal conflicts and grievances
ECOWAS (2020)	Regional policy	Violent extremism	West Africa	Joint operations constrained by political suspicion and capacity asymmetries
ENACT (2023)	Institutional index	Organized crime	Africa (all states)	Criminal markets embedded in the regional political economy; resilience varies by country
UNODC (2020; 2024; 2025)	Institutional reports	Organized crime	Africa; global	Firearms trafficking; trafficking in persons; drug transit and consumption
UNCTAD (2020); AU & UNECA (2015)	Institutional	Illicit finance	Africa	IFFs ≈ $89bn/yr (~3.7% of GDP), ~half from extractive mis-invoicing; earlier estimate $50–80bn
INTERPOL (2025; 2026)	Institutional reports	Cybercrime	Africa	Losses $192m (2024) →$484m (2025); AI in 55% of reported cases; ransomware detections by country
Abubakari (2021); Mensah (2023); Aphane (2025); Pieterse (2021)	Academic	Cybercrime; cyber governance	West/Southern Africa	Limits of cybercrime policy; victim impacts; policing capacity deficits; breaches eroding institutional trust
Ifeanyi-Ajufo (2023)	Academic	Cyber governance	Africa	Sovereignty–cooperation dilemma; weaponisation of cyber laws against dissent
ICC IMB (2026)	Institutional report	Maritime insecurity	Global; Gulf of Guinea	21 Gulf of Guinea incidents (2025), 23 crew kidnapped; 137 global incidents; weapons in >50% of attacks
ECOWAS (2025); UNCTAD (2024)	Regional / institutional	Maritime insecurity	West Africa	IUU fishing up to 40% of catches; losses $2.3–9.4bn/yr
UNCTAD (2025)	Institutional	Maritime	Global; Africa	Red Sea disruption raising insurance

		trade		and import costs for Africa
IDMC (2025)	Institutional report	Cross-cutting (displacement)	Sub-Saharan Africa	38.8m IDPs at end-2024; ~46% of global total
World Bank (2015; 2024); Charbonneau(2021); Döring(2023); Prah (2023)	Institutional / academic	Governance; security policy	Africa; Sahel	De-risking harms on remittances; FCV strategy; counter-insurgency governance; regional security arrangements
World Bank Group (2026); African Development Bank (2026); ECHO(2026); OCHA(2026); GCR2P-2026	Institutional	DRC case study	DRC; eastern provinces	Cobalt ~70% of world mined supply; 81.1% extreme poverty; IDPs 7.3–7.8m peak (2025) → ~5.8m (early 2026); 18.5m in need

Inclusion and Exclusion Criteria

Exclusion criteria: (1) publication outside of the 2020-2026 window (except canonical theoretical or benchmark works identified through snowball sampling, such as UNDP, 1994; AU & UNECA, 2015; World Bank, 2015; INTERPOL, 2021; IMB, 2021; IEP, 2021; IDMC, 2021; ENACT); (2)documents that were not directly relevant to one of the four threat domains in an African context;

(3) documents that were not published in English or provide an official English translation; and

(4) documents were not directly relevant to the four threat domains in a way that could be extrapolated from the existing English text.

Exclusion criteria: (1) geographic focus outside Africa (unless the work provides an explicit theoretical or comparative mechanism, as in Idler (2020) which was based in Colombia but was retained because it theorises the causal relationship between illicit flows and armed-group behaviour, which this study applies heuristically to African cases); (2) opinion pieces, commentaries, and unattributed media content without verifiable data; (3) superseded editions of recurrent institutional reports (only the most recent GTI, IMB, and INTERPOL editions at the time of search were retained, with earlier editions cited only for time-series comparison); and (4) sources presenting statistics that could not be verified against any independent source were excluded, or, where uniquely relevant, cited with an explicit caveat in the text.

Institutional sources were weighted by quality, according to the recommendations of stakeholders; methodological transparency, meaning that IDMC and IEP document the methods they use to collect data, and index-based sources were triangulated with at least one non-index source. If there is any significant difference between two data sources, such as the two displacement figures for eastern DRC, it is reported as such rather than as a single figure.

ANALYTICAL PROCEDURE

The analytical framework is based on Critical Security Studies (CSS) and Political Economy (PE) approaches, which look beyond the state as the sole security actor to citizens' experiences and emphasize the economic and institutional structures that underpin insecurity. Two steps of analysis were taken. The concepts in the conceptual framework below were applied deductively to code the material in the following order: first, the securitization paradox; second, human security; and third, the five-type convergence typology. Second, the patterns identified through inductive coding across the sources (crime–terror nexus, the land–sea linkage in maritime crime, and weaponization of cyber legislation) were refined iteratively. This is a reflexive thematic analysis (Braun & Clarke, 2022) that was attempted, but due to reliance on secondary sources and the absence of exhaustive, systematic coding, it is reported as a thematic synthesis.

The cross-cutting thematic claims of the study were tested with two named empirical cases, one representing the most severely affected country in the world by terrorism (the Sahel polycrisis, with a specific focus on Burkina Faso) and the other the most dramatic example of the crime–conflict–resource nexus in the region (the resource curse in the Democratic Republic of Congo).

Reflexivity and Limitations

The researcher adopted reflexivity as a method in the research procedure. The study recognizes the potential to create victim narratives and to provide a single-cause analysis of structurally complex crises. It deliberately juxtaposes information from African institutional sources (the African Union, ENACT, and national government evidence) with that from Northern policy sources to reduce epistemic imbalance in the evidence base. The study relies entirely on secondary data and cannot independently confirm or disconfirm any disputed data, such as the numbers of displaced people, which vary widely and frequently in eastern DRC; it also does not provide the detailed information that fieldwork or interviews with affected communities would provide. If sources differ significantly, the difference is noted and not reconciled by selecting the most convenient number. Future research that combines the desk synthesis with field or survey approaches would be useful for confirming and extending the conclusions reached on this page.

CONCEPTUAL AND THEORETICAL FRAMEWORK

These threats are transnational when their activities, financing, impacts, and responses are not contained within a single country. Threats are not limited to crossing borders but also involve networked patterns and thus require multiple actors to address them. Licit and illicit flows are often conflated in Africa, as borders intersect with trade areas, pastoralist mobility corridors, kinship networks, transport routes, and coastal livelihoods (Döring, 2023; Idler, 2020). This paper takes a Critical Security Studies (CSS) and Political Economy perspective, as opposed to the traditional state-centric realism.

Defining Threat Convergence

As convergence might become an unexamined label, the paper defines five analytical types of convergence and specifies a priori the types of convergence the claims apply to:

Type 1 — Multiple types of crime being committed by the same actors. JNIM imposes excise taxes on artisanal gold mining, kidnaps for ransom, forces zakat collection and livestock theft, and conducts insurgency operations (Africa Centre for Strategic Studies, 2025; GI-TOC, 2023). The actor is one; the criminalities are several.

Type 2 — Other actors working with the same infrastructure. Criminal networks and extremist groups use the same smuggling corridors, border crossings, mobile-money and informal value-transfer systems, fake documents and encrypted messaging; cyber infrastructure (SIM-boxes, compromised networks, crypto-mule accounts) is used by both fraudsters and traffickers, and extremist sources of finance (Muggah, 2023; Idler, 2020).

Type 3 — Enabling conditions shared with others. These governance failures—corruption, weak justice and accountability, limited regulatory and technical capacity, gaps in border management, financial opacity, and socio-economic exclusion—are essential to understanding the actions of different actors and their motives. This is the variable in the middle of the paper, which is mapped domain-by-domain in Table 2 below.

Type 4 — Causal relationships between domains. Other artisanal fishing activities are affected by IUU fishing, which in turn can lead to recruitment into piracy and trafficking (Type 4a), to displacement due to conflict, which exposes people to trafficking and recruitment (Type 4b), and to the proceeds of cyber-fraud being used to finance other illicit markets (Type 4c) (VreË, 2020; IDMC, 2025; UNODC, 2024).

Type 5 — Coincidence of occurrence. Cybercrime losses are increasing, whereas terrorism-related deaths are decreasing, as revealed by data from 2024-2025 (INTERPOL, 2026; IEP, 2026). The paper does not claim that the co-occurrence is necessarily a temporal coincidence, and provides no clear evidence of actors or infrastructure, nor of causality.

The central thesis of the paper, that the four domains are not analytically separable, should thus be read in the context that the domains are interconnected via Types 1-4 and that it is Type 3 (shared governance deficits) that provides the common explanatory structure. Where there is conceptual overlap, it is not considered a sign of convergence; each alleged convergence is linked to at least one of the four substantive types and to the sources listed in Table 1.

The Securitization Paradox, Human Security and Regional Interdependence

In African countries, transnational threats are generally perceived as threats to the state and thus as requiring extraordinary action, such as military action. This leaves behind the 'securitization paradox ': citizens are not always secure when the state deploys security actors. Rights abuses and collective punishment in the Sahel result from coercive operations, leading to a lack of trust and intelligence cooperation, and ultimately to instability (Charbonneau, 2021). The rule of law applicable to borders, finances, technology, and markets (governance) is undermined by governance institutions that are more engaged in territorial control than in the protection of citizens, and by corruption and discrimination that detract from the trust of citizens in the system and invite the exploitation of governance gaps by non-state actors (Döring, 2023).

To address this paradox, this paper will use the human security framework (UNDP, 1994), which shifts the referent of security from the state to the person. Not only to the military but also to the immediate realities of populations – fear, displacement, loss of livelihood, denial of legal protection – and security is not defined as the absence of conflict, but as the existence of justice, service delivery, and economic opportunity (UNDP, 2023), which is corroborated by empirical research on recruitment in Africa.

The security situation in these regions is interlinked; crises spread from one state to another via migration, arms transfers, trade, and financial transactions, as illustrated by the Sahel, the Lake Chad Basin, the Horn of Africa, and the Red Sea Corridor. Regional mechanisms should therefore reinforce, not supplant, good national governance; they should not replace military intervention but rather embrace full cooperation to address vulnerability drivers and ensure that joint operations at the borders support human rights protection and judicial strengthening (Döring, 2023).

Hybrid Threat Networks

Types 1 and 2 above are the most common threat network types that combine to form a hybrid threat network, enabled by Type 3. Consequently, there are notable grey zones between violent extremism and organized crime, cybercrime and maritime insecurity: violent groups are extorting smugglers, other criminals extorting merchants, and weapons being acquired from criminal networks that involve corrupt port and customs officials. These overlaps do not mean that actors or motives are fully interchangeable, but rather constitute evidence of a deep-rooted political economy of violence in which the lines between criminals, armed actors, and political actors become increasingly blurred (Idler, 2020; Muggah, 2023). However, multi-agency measures involving law enforcement, customs, financial intelligence agencies, maritime authorities, cyber experts, prosecutors, and social services, all tailored to ensure that no individual is arbitrarily coerced and that privacy rights are not breached, are necessary to address such hybrid threats. The challenge is illustrated by the case of cyberspace governance, where defending the state does not imply compromising cross-border cooperation that the effective security of cyberspace demands (Ifeanyi-Ajufo, 2023).

FINDINGS AND DISCUSSION

Violent Extremism and Terrorism

Violent extremism is still a significant trans-border issue: affiliates of Al-Qaeda and the Islamic State are present in the Sahel, Lake Chad Basin, Horn of Africa and northern Mozambique. It is a mistake to view the situation solely as an ideological matter and/or as a global terror threat; the strength and survival of these communities depend on local grievances, social marginalization, illicit economies, and the lack of state (Thurston, 2020; Zenn, 2020). The threat is as real as it can be: The Global Terrorism Index (GTI) 2026 reports that the Sahel accounted for more than half of all global deaths caused by terror in 2025, with global deaths from terrorism falling 28 percent year-on-year to 5,582, the lowest since 2007 (IEP, 2026). Almost three-quarters of all terrorism fatalities in 2025 were seen in only five nations – namely, Pakistan, Burkina Faso, Nigeria, Niger and the DRC – a focus that has narrowed both regionally and internationally (IEP, 2026).

Political economy of rebellion and regional expansion. Arms, capital, information, and manpower flow in the Sahel are vital to terrorist operations. Borders, which once signified the end of the state's administrative reach, are now giving armed groups strategic room to maneuver: to retreat, regroup, and escape military pressure by exploiting jurisdictional blind spots. Regional bodies like ECOWAS have agreed on the need for coordinated joint operations, but limited intelligence sharing stems from mistrust, political suspicion, unequal institutional capacity, and conflicting national interests among partners (ECOWAS, 2020).

The financial system of the most dominant militant group in the region – Jama'at Nasr al-Islam wal Muslimin (JNIM) in Mali, Burkina Faso, and Niger – reflects the political economy of rebellion. JNIM is diversifying from external sponsorship, operating at least four distinct sources of illicit revenue: taxation and/or control of artisanal gold mining (with annual reported production worth tens of millions of USD in areas under its control); kidnapping for ransom, which grew by approximately 30x in Burkina Faso between 2017 and 2022 as recruitment expanded; forced collection of zakat; and livestock theft (estimated to cost Mali several billion CFA francs in recent years [Africa Center for Strategic Studies, 2025; Global Initiative Against Transnational Organized Crime [GI-TOC], 2023]). This is a nominally ideological insurgency that functions as a rent-extracting criminal enterprise, run in conjunction with local trade, pastoral, and mining economies – a pure form of Type 1 convergence.

Similarly, the Boko Haram and Islamic State West Africa Province (ISWAP) movement in the Lake Chad Basin attests to the local nature of transnational jihadist ideology, which adapts to prior communal conflicts, resource deprivation, and political discontent (Zenn, 2021: 41). Interweaving external relations and close local links puts the group into the social fabric of the region, making them resilient. But preventive measures cannot be based solely on a military containment approach; they must also be integrative, incorporating robust national and regional institutional support, localized conflict resolution, and community engagement (Döring, 2023).

Loss of life and displacement of people, and the loss of state legitimacy. The first impact of violent extremism is the systematic disruption of civilian life and the deterioration of the local socio-economic fabric. Terrorist attacks are directed at specific areas where normal community life takes place, such as markets, schools, clinics, transport systems, places of worship and local government offices. When people are insecure in the long term, a domino effect occurs, and essential functions begin to disappear, such as farmers leaving the land, traders reducing their movement, children not attending school, and health professionals leaving the country. In addition to the deaths, this destruction diminishes communities' ability to manage and recover from crises and their social and economic autonomy (UNDP, 2023).

These disruptions result in mass displacement and, in turn, a vicious humanitarian cycle (Type 4 causal linkage). There is a connection between violence and loss of livelihoods and public services – people also run for these. IDPs are at a high risk of secondary exploitation such as trafficking and gender based violence in transit and camps, and host communities face high pressure on land, water, education and labour markets. A lack of livelihoods programming and social cohesion can lead to inter-communal tensions, in which a localized security crisis becomes a regional fragility (IDMC, 2025).

Importantly, the State's response compounded the legitimacy problem. It is not uncommon for civilians to be caught in the crossfire of conflict, both from non-state armed groups and from overly militaristic security forces. The implementation of coercive counter-terrorism measures, including arbitrary detention, collective punishment, ethnic profiling and extrajudicial violence, may provide tactical compliance in the short term, but undermine civilian trust, which is essential for long-term stability. Respecting human rights and protecting civilians is a moral, legal, and strategic duty: if there is no local intelligence to be gained, a state without the goodwill of its citizens cannot obtain it to dismantle transnational extremist networks.

Structural, political and economic implications. Violent extremism weakens political structures and reveals the precarious nature of the state's monopoly over violence. In the Sahel, military coups have been achieved by exploiting security lapses: Mali (2020 and 2021), Burkina Faso (twice in 2022), and Niger (2023) all saw a military coup, all of which were explicitly linked to the counter-terrorism threat, with a subsequent shift in focus toward Russian security cooperation. In the past, civilian governance has been replaced by military juntas with little to no improvement in security outcomes, as they tend to reduce civic space, curtail international relations, and erode public trust, which is crucial for counter-insurgency (Prah, 2023).

The economic cost is also significant. Insecurity increases transport prices, negatively impacts pastoral and agricultural value chains, scares off foreign direct investment, and diverts public resources from long-term development to emergency response. A localized insurgency has devastated livelihoods and is impacting multi-national investments in the natural gas sector in Cabo Delgado, Mozambique, highlighting how localized violence can spread into global supply chains (World Bank, 2024). Security can therefore not be effective alone; it has to be linked to governance and socio-economic inclusion, as existing marginalization, exclusion and humiliation can create fertile grounds for extremist networks to grow.

Transnational Organized Crime, Trafficking and Illicit Economies

Transnational organized crime (TOC), be it narcotics, human trafficking, weapon smuggling, illegal mining, wildlife poaching, money laundering, fuel diversion, or corruption of state institutions, costs huge illegal profits and makes it difficult for legitimate markets. The Africa Organized Crime Index reveals that these organized criminal markets are not specific to post-conflict areas but rather are a by-product of the regional political economy, which varies significantly in its effects on countries' resilience (ENACT, 2023).

The dynamics of TOC are not only criminal, but a combination of survival and exploitation. Illegal market activity creates an informal safety net for marginal livelihoods, which in turn raises the risk of violence and the political power of criminal gangs in the context of low employment opportunities in the formal sector and low levels of public services. This is part of the reason why low-level enforcement actions so frequently fail to stop crime: they do not eradicate crime but merely displace and adapt criminal systems (Gutierrez, 2020). TOC is thus more than just a money-maker – it encourages corruption, it nourishes more violence, and it weakens the institutional capacity needed to achieve sustainable development.

Illegal markets, corruption and institutional capture. Syndicates regularly recruit state officials from customs, police, immigration, and municipal services through bribery, coercion, or complicity, maintaining complex logistics systems through regular operations that include transporting, storing, financing, documenting, and physically protecting the goods (Muggah, 2023). The greatest threat is institutional capture, in which criminals' gains will undermine the regulatory and protective role of the state.

The harm is exacerbated by illicit financial flows (IFFs) that rob countries of funds and bring dirty money into the mainstream global economy. According to UNCTAD (2020), Africa is losing around USD 89 billion annually to IFFs, close to 3.7 percent of the continent's GDP, of which nearly half is lost due to misinvoicing of commodity exports, primarily gold, diamonds, and platinum. A previous estimate by the African Union/UNECA High Level Panel (2015) placed the range at USD 50-80 billion per year. Both of these are more than the official development assistance for the whole continent in a year, and the money that remains could fill a significant portion of the estimated USD 200 billion annual funding deficit to meet the Sustainable Development Goals. These networks can be broken through arresting low-level couriers, but only with the help of complex financial investigations, forced beneficial-ownership transparency, asset seizures, and cross-border coordination — and some concern for the underlying factors, such as demand for illegal products in the Global South and the enabling role of the Global North financial networks. (Idler, 2020)

Drug, person and firearm trafficking. Africa is both a transit point and a consumer market and, in some instances, a source market for global illicit trades. Narcotics: the continent's contribution to the trafficking of drugs, particularly cocaine, heroin and synthetics; it contributes to corruption, empowers violent syndicates and robs public health resources; a response can be effective by means of intelligence sharing, financial monitoring and public health measures (UNODC, 2025). Trafficking in persons: criminal networks capitalize on armed conflict, gender inequality, climate change, and economic deprivation to traffic people to be exploited in forced labour, sexual exploitation, and domestic servitude; responses need to extend beyond prosecution and include a human rights-based approach that emphasizes victim protection, psychosocial services, and safe and legal migration opportunities (UNODC, 2024). Small arms and light weapons are a source of criminal enterprise and extremist violence, and conflicts are more deadly locally because of the availability of these weapons; tracing of such weapons; diversion prevention; control over local stockpiles; and extensive cross-border cooperation are needed to mitigate the effects of these weapons (UNODC, 2020).

The crime–terror nexus and illicit finance. Organized crime and violent extremism in Africa are more pragmatic, transactional and situational, and less ideological: armed groups collect taxes from smugglers and ensure the smooth functioning of the illicit trade, while syndicates leverage unstable environments to divert the the attention of state enforcement agencies (Muggah, 2023). If you want to disrupt this symbiotic relationship, you need to go after its blood — cash, cash, cash! Implementation of counter-terrorist financing (CTF) creates a policy paradox: risk-based regulations; cooperation across borders; and asset recovery are necessary, but de-risking of global financial institutions has been demonstrated to cut off legitimate remittance flows and to negatively affect fragile economies, civil society, and humanitarian operations (World Bank, 2015). Financial regulations that are not specifically aimed at the very vulnerable members of society could negatively affect the very people resilience programmes aim to help, so precise, evidence-based, and well-calibrated regulation is needed.

Cybercrime and Digital Insecurity

Cybercrime is a trans-border activity that is constantly changing: the offenders are spread out, the victims are scattered, so are the servers, payment systems, and proceeds, and attribution, investigation, and prosecution are extremely hard. Phishing, business email compromise, ransomware, identity theft, and mobile money scams represent major and emerging issues across the continent of cybercrime and fraud (INTERPOL, 2025). As digital transformation continues, exposure is growing across Africa, where digital transactions will surpass USD 1.1 trillion by 2025, and over 570 million individuals are already internet users, with mobile subscriptions reaching over 1.1 billion (INTERPOL, 2026). According to INTERPOL's African Cyberthreat Assessment Report 2026, artificial intelligence (AI) is responsible for half of the cases reported, with a number estimated at 55 percent; AI is being used for tasks such as automating phishing, creating a synthetic identity and deepfaking biometric information, which is capable of bypassing bank verification systems, and is predicted to result in an increase in financial losses, with measured losses rising from USD 192 million in 2024 to USD 484 million in 2025.

Cybercrime is not just a technological or IT issue; it affects rust in Africa's emerging digital economy, public institutions, and in international business relations. Financial loss is not only significant in terms of monetary damages, but the reputational impact is also large, resulting in tighter security and compliance measures by financial institutions and payment providers that can serve as barriers to financial inclusion, increase transaction costs, and decrease confidence in e-commerce and digital governance (Abubakari, 2021).

The growing attack surface and the asymmetry of infrastructure in the digital world. The poorest are the ones most likely to suffer the greatest losses. Small and medium-sized enterprises (SMEs) in particular are vulnerable due to a lack of infrastructure, a shortage of specialized cybersecurity skills, and a lack of cyber insurance. The number of ransomware detections is a testament to the continent's most digitized economies: South Africa saw 17,849 reported ransomware attacks in one year alone, Egypt 12,281, Nigeria 3,459 and Kenya 3,030 (INTERPOL, 2025), including in critical infrastructure and government databases such as the Kenyan roads authority and Nigeria's national statistics agency. The fraud and ransomware victims not only suffer financial losses but also have their lives disrupted, see compliance costs rise, and suffer psychological damage (Mensah, 2023).

The rapid digitization of public services — taxation, procurement, healthcare, education, civil registration, border control, and electoral systems — has multiplied the state's attack surface. The leakages of public sector systems not only risk their ability to deliver services effectively, but also affect sensitive citizen data, privacy, and public confidence in public sector institutions, as the South African experience demonstrates, having a direct impact on public trust in public sector institutions and affecting a sense of governance and legitimacy (Pieterse, 2021).

Economics, misinformation and democratic strength. In addition to actual theft, a general culture of cyber fraud undermines national reputations, which in turn scare off investors, correspondent banks, and foreign clients by compromising the trustworthiness of domestic digital markets (Abubakari, 2021). Meanwhile,, the Digital Ecosystem is becoming a weapon through the spread of fake information. While a definition of disinformation may not be a cybercrime per se, it thrives in the same digital setting of vulnerability, inadequate verification, and declining trust. Electoral or protest rallies, or emergencies involving public health, conducted in an uncoordinated manner contribute to polarization, undermine democratic processes and delay crisis responses. This dual threat has shifted cyber governance from a technical issue to a matter of national sovereignty and 'cognitive security,' and points to the need for robust regional cooperation to protect the informational integrity and the democratic resilience of the state (Ifeanyi-Ajufo, 2023).

Rights and regional coordination, cyber governance. Though many African countries have enacted cybercrime and data protection laws, they are significantly hampered by capacity limitations: investigators are poorly equipped and trained, courts have limited experience with electronic evidence, and public digital security awareness is low. Continued investments in expertise, institutional capacity, and international cooperation are needed (Aphane, 2025). Deliberate abuse is a big part of the problem, and one of the paradoxes of the current cyber governance landscape in Africa is the way cyber laws are being used to jail critics, monitor journalists, and suppress opposition by defining cybercrime, misinformation, or hate speech under the laws. Cyber governance, then, should be very careful not to confuse actual malicious activity with legitimate freedom of expression, integrating independent judicial review, and should be grounded on digital human rights, since effective security can only be achieved through citizen cooperation. One that ignores civil liberties is strategically self-defeating: it can alienate the citizen cooperation that is essential to achieving effective security (Ifeanyi-Ajufo, 2023).

Maritime Insecurity and Illegal Blue Crime

Maritime security includes piracy, armed robbery at sea, illegal, unreported and unregulated (IUU) fishing, oil

bunkering, human trafficking and corrupt port operations. Its transnationality is built in: everything from vessels to crews, insurers, ports, and criminal syndicates crosses multiple maritime jurisdictions, and thus no single country's response is enough (Bueger, 2024). Maritime security is not only about naval security but also law enforcement, commercial logistics, environmental protection and international diplomacy.

Political economy of the coast, IUU fishing and piracy. Port integrity, availability of fuel supplies, financial networks, access to markets, and local security systems are all influencing factors on shore for criminal operations at sea. This land–sea nexus has ensured that 'offshore enforcement, without onshore governance' is just a symptom – action to mitigate requires a combination of maritime enforcement, port security, sustainable fisheries management, criminal justice reform and development of legitimate coastal economies' (Vreÿ, 2020).

It not only threatens the safety of seafarers but also slows down shipping and increases global insurance rates through piracy and armed robbery at sea. The Gulf of Guinea is a good example of how the threat is persistent despite the low-level headline figures: in 2025, the IMB recorded 21 incidents in the region, with 23 crew members kidnapped in four separate attacks and three other hostages taken and one crew injury (ICC International Maritime Bureau [IMB], 2026). The number of piracy and armed robbery incidents reported to the IMB in 2025 increased to 137, though such cases appear to be increasing in severity, as weapons were used in more than half of all reported incidents, the highest percentage since 2017 (IMB, 2026). How localized maritime insecurity can have a knock-on effect on global shipping routes and international trade is evident in the persistent vulnerabilities in the Gulf of Guinea, the Red Sea and the Gulf of Aden.

However, an exclusive attention to piracy ignores a more fundamental cause – IUU fishing. Fishing fleets, operating at a distance, systematically exhaust local fish stocks, limiting food security, environmental protection, and the regulatory capacity of coastal countries. Up to 40 percent of the catches in parts of the Gulf of Guinea are estimated as illegal, resulting in an estimated loss of USD 2.3–9.4 billion annually to West African economies, of which the Commissioner for Political Affairs, Peace and Security of ECOWAS has estimated at more than USD 2 billion per year, with direct consequences for livelihoods and security (ECOWAS, 2025). This ecological and economic destruction places the livelihoods of these artisanal fishing communities at risk. It renders the alternatives of smuggling, piracy and trafficking more attractive to these grassroots coastal communities. IUU fishing is therefore not only an environmental crime but also a structural catalyst for maritime crime (Type 4 causal link), and coastal resilience and sustainable fisheries management are part of Africa's security policy (UNCTAD, 2024; Vreÿ, 2020).

Fragmented governance and economic impacts. Sea transport supplies 96% of Africa's trade, making it extremely vulnerable to disruption. Maritime insecurity leads to increases in insurance costs and adds to the cost of rerouting world trade, including in the Red Sea, for critical imports like food and fuel (UNCTAD, 2025). These shocks are a structural tax on development, costing disproportionately to countries without access to the sea and coastal communities reliant on reliable supply lines. The impact on people is also devastating: seafarers are injured, kidnapped and killed, and local people suffer direct loss of income from illegal fishing and piracy. Marginalized coastal youth seek opportunities in the black economy at sea where the linkage between the illegal economy at sea and governance shortfalls and poverty onshore is direct (Vreÿ, 2020).

The issue of jurisdictional fragmentation exacerbates the situation – a single ship can be operated under a flag of convenience in one country, owned in another, and attacked in the territorial waters of a third country. Divergent requirements, varying national capacities, conflicting laws, and poor information sharing provide opportunities for maritime syndicates (Okul, 2026; Williams, 2021). Maritime security in areas such as the Western Indian Ocean is thus not possible without strong regional governance frameworks that can address the aforementioned asymmetries.

Towards an integrated blue economy security framework. Aside from maritime domain awareness and naval patrols, there is a need for other solutions. An Integrated Maritime Security approach accepts that the security issue for the sea is, in fact, the security issue for the land: where maritime security is absent or, at best, substandard, courts are unable to prosecute criminals and coastal people are economically marginalized. A comprehensive approach should thus connect maritime security and port security, anti-corruption efforts, sustainable fisheries, and a sustainable and legitimate coastal economy to overcome the land-sea divide (Bueger, 2024). This needs to be done through deep regional cooperation – joint patrols, common information platforms, mutual legal assistance – fueled by political will, clear mandate, and realistic understanding of asymmetric state capacities (Williams, 2021). Finally, the protection of the maritime domain is a governance project that engages economics, justice and regional solidarity.

CROSS-CUTTING IMPACTS: THE SECURITY-DEVELOPMENT NEXUS

The post-colonial African state is under attack from all three fronts – violent extremism, organized crime, cybersecurity and maritime piracy. They are separate but strongly interconnected and help create compound crises of mass displacement, affected regional trade, institutional decay, and general mistrust. All spillovers are multi-layered: pressure on host communities due to the refugee flows, capital flight and economic instability, transnational spread of criminal and radical networks, and the further spread of illegal arms that contribute to ongoing conflict. Security policy is no longer manageable within the Defence or Interior Ministries, but should be embedded in development planning, the provision of social welfare, Justice sector reform, and regional diplomacy. Addressing them separately hides the common Type 3 root causes and perpetuates the illusion that there are short-term coercive fixes which will not address structural issues.

Identifying areas of Shared Governance within the Four Threat Domains

Table 2 clarifies the four domains “targeting the same underlying governance deficits.” Six deficits are identified, and for each, there is a mechanism connecting it to each threat domain, accompanied by an evidentiary anchor. The mapping reveals that the deficits are common but act in different ways, through domain-specific processes — hence why an integrated, governance-based approach beats domain-siloed coercion.

Table 2: Mapping of shared governance deficits to threat domains (Type 3 convergence), with mechanisms and evidence

Governance deficit	Violent extremism	Organized crime	Cybercrime	Maritime insecurity
Corruption & institutional capture	Complicit officials inform and supply insurgents; security-sector abuses drive recruitment	Bribery of customs/police/immigration sustains trafficking networks (Muggah, 2023)	Complicit insiders enable SIM-registration and identity fraud	Corrupt port and customs officials underpin the land–sea nexus (Vreÿ, 2020)
Weak justice & accountability	Impunity and arbitrary detention fuel grievances and intelligence loss (Charbonneau, 2021)	Low prosecution rates for kingpins; networks adapt after crackdowns (Gutierrez, 2020)	Courts lack capacity to handle electronic evidence (Aphane, 2025)	Very low arrest-to-prosecution ratios for piracy and IUU offences
Limited regulatory & technical capacity	Absent state presence in peripheral rural areas (Thurston, 2020)	Beneficial-ownership and asset-recovery laws unenforced (Idler, 2020)	No forensic/CERT capacity against AI-enabled fraud (INTERPOL, 2026)	Weak monitoring, control and surveillance of fisheries (ECOWAS, 2025)
Border-management gaps	Cross-border arms and fighter movement sustains the Sahel insurgency(ECOWAS, 2020)	Smuggling corridors across porous borders (ENACT, 2023)	Jurisdictional fragmentation impedes attribution and MLATs	Flag/ownership/attack jurisdictions split across states (Okul, 2026)
Financial opacity & illicit flows	Gold and ransom revenues laundered through informal channels (GI-TOC, 2023)	Trade mis-invoicing: ~$89bn/yr in IFFs (UNCTAD, 2020)	Mule accounts and crypto obfuscate proceeds	Laundered proceeds of fish and oil theft enter formal economy (UNCTAD, 2024)
Socio-economic exclusion	Marginalisatio n and humiliation drive recruitment (UNDP, 2023)	Illicit economies serve as informal safety nets (Gutierrez, 2020)	Low digital literacy raises victimisation and limits reporting	IUU-driven livelihood loss feeds piracy recruitment (Vreÿ, 2020)

Three observations follow. First, there is crossover among corruption, border gaps, and financial opacity across all four domains, the strongest convergence channels. Second, the mechanism is different for each of the domains: what causes recruitment in the violent-extremism column causes adaptation and displacement in the crime columns. Third, the explanation of this empirical regularity, which is clearly seen in Table 1, is the reason for not considering the co-occurrence of Type 5 as a single fused threat system: states with the weakest scores across the six deficits (Sahel states, DRC, coastal West Africa) also have the most severe scores across all four threats.

Human Security and Displacement

'The state's failure to keep citizens safe and to ensure vital services is best measured by mass displacement.

Secondary risks, such as recruitment by armed groups, human trafficking and exploitation, affect both displaced and host communities, while heavy socio-economic burdens are assessed on host communities. Human-security interventions must therefore do more than merely provide relief in the needy's time; they must also secure legal documentation, access to healthcare and education, psychosocial support, and livelihood recovery, prevent the intergenerational transmission of trauma and vulnerability, and re-establish the social contract between state and citizen (IDMC, 2025).

State Legitimacy, Democratic Resilience and Regional Cooperation

Governments can invoke transnational threats to bolster their security agenda and expose serious shortcomings in the performance of policing, justice and financial systems, while paving the way for corruption and authoritarian drift. When the state is a predator rather than a protector, it begins to violate the social contract: citizens will not report dangers or help intelligence services when they perceive such state action as a violation of their civic liberties. There is, therefore, a need to safeguard human rights while building institutional capacity to ensure effective governance of digital and transnational security; measures that compromise public trust are counterproductive (Ifeanyi-Ajufo, 2023).

Deep-level cooperation is also critical and challenging. For the success of intelligence sharing, mutual legal assistance, harmonized laws, and joint investigations, states need to understand the interdependence between national security and the stability of their neighbours. Regional programmes are most effective if they build resilience and legitimacy, and strengthen national systems and regional protection mechanisms (Prah, 2023).

EMPIRICAL CASE STUDIES: VALIDATING THE GOVERNANCE-SECURITY NEXUS

Violence, illicit finance, and governance failure are evident globally in two of the most striking and information-dense crises on the continent today. Two cases of validation are presented as examples: the Sahel polycrisis (focused on Burkina Faso) and the resource curse in the DRC, the world's most terrorism-burdened and the continent's most complex country on the crime-conflict-resource axis, respectively.

Burkina Faso and the Sahel Polycrisis

Burkina Faso offers the starkest illustration of the securitization paradox. It was the worst country in the world to be a victim of terrorism for two years in a row (2023 and 2024) and had approximately a quarter of all global terrorism deaths in 2023 (1,907 deaths compared to 1,135 deaths in 2022, IEP, 2024). Burkina Faso was consistently the country most impacted by terrorism, with deaths dropping by 21 percent in 2024 to 1,532, and then by another 45 percent to 846 in 2025 (IEP, 2025, 2026). At first glance, it seems a triumph for security. Still, the Global Terrorism Index 2026 advises against reading too much into it, because security gains could be short-lived if access to basic services is limited, continuing abuses of the security forces are unchecked, and extreme poverty is left unaddressed.

This is evident in the political economy of the insurgency. JNIM has created a diversified illicit war economy: it taxes and controls artisanal gold-mining sites that generate an estimated tens of millions of US dollars per year in the areas it holds; ransom payments for high-value hostages have reportedly run into the tens of millions of dollars; and cattle theft — a traditional criminal economy in the Sahel — has been estimated to cost Mali several billion CFA francs (Africa Center for Strategic Studies, 2025; GI-TOC, 2023). The military takeovers in Mali (2020, 2021), Burkina Faso (twice in 2022), and Niger (2023) on counter-terrorism grounds, their shifts in security cooperation from France to Russia, and their impact on civilian trust and on international intelligence-sharing platforms that underpinned counter-insurgency capacity all contributed to tensions.Several military coups in Mali (2020, 2021), Burkina Faso (twice in 2022), and Niger (2023) on counter-terrorism grounds, their turn to Russia for security cooperation, and the impact on civilian trust and on international intelligence-sharing platforms sustaining counter-insurgency capacity all created tensions. The outcome — as the paper's central thesis — is that a significant decrease in lethality has not led to the alleviation of the governance vacuum: the number of terrorist attacks has been reduced, but their structure has not changed, and they have spread into the previously less-affected coastal states of Benin and Togo, which will see approximately 3,000 more troops deployed to their northern border in 2025 (IEP, 2026).

Democratic Republic of Congo: Resource Wealth, Armed Conflict, and the Limits of Extraction-Led Development

The DRC is a structurally distinct but analytically similar process: a mineral-rich, conflict-stricken nation where resource largesse can be used to consolidate insecurity and elite control rather than to represent a more general process of development. Cobalt is a major commodity, with production contributing more than 30 percent to national budget revenue, and mining (primarily copper and cobalt) contributing more than 30 percent to national production, the majority of which is sold on the international market (African Development Bank, 2026; World Bank Group, 2026). However, the same level of mineral abundance is associated with high levels of deprivation: according to the World Bank Group (2026), in 2025, 81.1 percent of people in Congo lived below the $3-a-day PPP poverty line, while the capital-intensive mining sector created very few jobs. Even though copper and cobalt exports continued to constitute the main source of foreign exchange earnings that helped to stabilize the Congolese franc later in the year, the cobalt sector has high governance stakes, as illustrated by the government's suspension of the exports (World Bank Group, 2026).

The eastern provinces (North Kivu, South Kivu and Ituri), which are host to much of the country's mineral wealth, have become the epicentre of one of the world's largest displacement crises. An estimated 100 armed groups operate in the region, including the Rwanda-backed March 23 Movement (M23), whose new offensive seized the provincial capitals of Goma (January 2025) and Bukavu soon after. There was a significant fluctuation in the levels of displacement, reaching approximately 7.3–7.8 million IDPs in 2025, the highest ever recorded in the country, and down to an estimated 5.8 million in early 2026, when an estimated 1.9 million people returned to their homes in North and South Kivu, only to find their homes destroyed or occupied (European Civil Protection and Humanitarian Aid Operations [ECHO], 2026; Global Centre for the Responsibility to Protect, 2026). An estimated 18.5 million Congolese need humanitarian assistance by 2026 (OCHA, 2026). It is instructive how this volatility is analogous to the maritime land–sea nexus, where the prize is control of extractive rents, not ideology: displacement in a resource-driven conflict doesn't even smooth out when violence subsides; it oscillates in and out with shifts in the armed actors' territorial control of extractive rents.

Comparative Lessons and Validation

The two cases, read together, provide a structurally different way to substantiate the paper's cross-cutting thesis. Hooded artisanal mining, livestock, and human movement (Type 1 and 3) are severely challenged by an ideologically driven insurgency in Burkina Faso, which has developed into a long-term illegal economic activity. In the DRC, the population does not benefit from a formalized extractive economy because it fails to ensure the availability of public services (Types 3 and 4), and armed groups claim rents before they reach the population. In both cases, the state's coercive response – the juntas and foreign military provocations in the Sahel, and the FARDC offensives and the UN's MONUSCO mission in the DRC – has brought back, at best, temporary and reversible gains, with no solution to the governance problems. The findings on displacement also apply to both situations: in the Sahel, displacement was slow-building, and in the DRC, it was sharp and even reversed in line with the movement of a single armed group, both of which indicate that any stabilization gains are very fragile without institutional reform. Both cases affirm the following: Africa's transnational security is not solely a military issue; neither is it a governance issue; and the two are not mutually exclusive. The two cases reinforce the following: Transnational security in Africa is not only a military matter; it is not only a governance question; and it is not a separate one.

STRATEGIC RECOMMENDATIONS: FROM COERCION TO GOVERNANCE

From Coercion to Service-Oriented Security and Accountability

African responses must transition from traditional military and coercive solutions to structural solutions grounded in governance – professional policing, independent judiciaries, secure civil registration, and efficient border management. The state's role in border and coastal areas, the epicentre of transnational security networks, should be understood not as one of surveillance and coercion, but as one of service, justice and protection, with a service-oriented approach in security and prevention building trust among the public, which is essential for cooperation (World Bank, 2024). Security policy and counter-terrorism measures must be based on intelligence, be proportionate,, be subject to independent,, rigorous oversight, and include civilian protection and meaningful community involvement in all actions. Effective accountability mechanisms are a human rights duty and a long-term strategy to prevent armed-group recruitment: the most effective way to prevent armed-group recruitment in the long term is through addressing root grievances through legitimate institutions (Charbonneau, 2021).

Disrupt Illicit Finance and Strengthen Accountable Justice Systems

Too often, the focus in anti-crime policy has been on eliminating the low-level couriers, but it should be on the structural enablers of illicit markets, including strong financial intelligence units, enforced beneficial ownership registries, cross-border asset recovery, specialized prosecutors, and robust witness protection (Idler, 2020). There is a need for institutional capacity—rights-respecting law enforcement and independent judiciaries—to address sophisticated economic crime (World Bank, 2024). Meanwhile, financial controls have to be proportionate and evidence-based, as excessive de-risking and CTF requirements destroy humanitarian organizations, remittance systems, informal economies and civil society, and thus impact on the resilience of those they serve (World Bank, 2015). African governments should leverage regional groupings to gain more bargaining power in international financial standard-setting institutions, without giving informal sector and legitimate remittances a competitive disadvantage. There is a need for independent civilian oversight of all counter-terrorism and anti-crime initiatives: the disruption of finances and the reform of justice systems based on human rights and due process leave no room for the development of illegal networks and, at the same time, maintain the citizen trust and confidence on which security cooperation relies.

Secure Digital and Maritime Spaces through Rights-Based Frameworks

Cyber resilience should be considered a key public asset, with a strong government security system, skilled judicial investigators, public awareness, and broad cooperation with technology and financial companies. Technical capacity, however, should be based on a rights-based approach: cyber laws must not criminalize dissent; evidence exchange and incident-response processes at the regional level must not violate privacy and freedom of expression. Cyber governance is successful when cybersecurity concerns are not used as weapons against civil society and when digital human rights are upheld (Ifeanyi-Ajufo, 2023).

Maritime security also needs to extend beyond the naval sphere to address structural causes of crime in the marine environment, including strict enforcement and port integrity, sustainable fisheries management, anti-corruption measures, prosecutions of offenders, and prioritized coastal community development. IUU fishing threatens local livelihoods, and security policies need to provide alternative legal activities for marginalized coastal communities, reducing their vulnerability and dependence on criminal activities (Bueger, 2024).

Deepen Regional Ownership and Local Prevention

Regional cooperation agencies like ECOWAS, SADC and IGAD must not only be given time to conduct ad hoc military operations but also be provided with effective institutions for intelligence sharing, mutual legal assistance, joint investigations and harmonized legal standards. However, without local ownership, technical cooperation cannot be effective: borderland and coastal populations are the first to be hit by transnational threats and must be given the floor as active members of the early warning and prevention process, rather than be considered as objects of state security (Döring, 2023; Prah, 2023). Prevention also needs to consider the structural drivers by investing in education, economic opportunity, social service delivery, and inclusive conflict resolution, thereby decreasing the use of violence and crime as economic tools or protective mechanisms. Security is sustainable where public institutions are viewed as more reliable than armed actors or criminal networks; when the risks of security are prevented at the local level, through human-centric approaches and the linking of regional epistemic cooperation, there is a much greater chance of addressing root causes of conflict rather than symptoms (Gutierrez, 2020).

CONCLUSION

Violent extremism, organized crime, cyber insecurity, and maritime piracy are all forms of governance failure in Africa and structural inequalities in the world. These threats are different in shape but are connected, in terms of actors, infrastructure, enabling conditions, and causal effects, into compound crises that weaken state institutions, fuel mass displacement, impact regional trade, and undermine the degree of trust between citizens and the state. But mere contemporaneity of trends is not convergence: the analysis has been intentionally limited to the first four types of connections which are demonstrable.

The answer is not to have more repressive security forces, or to militarize borders, but to fundamentally change governance. True security is built on accountable institutions, equitable access to justice, financial transparency and the strict protection of human rights. The evidence presented here makes it clear that rights-based policies that boost public authority and socio-economic inclusion can do far more than force to restrict the operational space of criminal and violent networks. The four domains are reliant on the same lack of governance and therefore can't be treated in isolation: transnational security in Africa is interdependent with the broader effort of inclusive and democratic governance.

REFERENCES

1. Abubakari, Y. (2021). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. Social Space, 21(1), 137–158.
2. Africa Center for Strategic Studies. (2025). Funding terror: How West Africa's deadly jihadist groups finance their operations.
3. African Development Bank. (2026). Critical minerals insights: Cobalt factsheet.
4. African Union & United Nations Economic Commission for Africa. (2015). Illicit financial flows: Report of the High Level Panel on Illicit Financial Flows from Africa.
5. Aphane, M. P. (2025). Policing cybercrime in South Africa: Issues and challenges. International Journal of Research in Business and Social Science, 14(6), 415–421.
6. Braun, V., & Clarke, V. (2022). Thematic analysis: A practical guide. SAGE.
7. Bueger, C. (2024). Securing the seas: A global agenda for maritime security. United Nations Institute for Disarmament Research.
8. Charbonneau, B. (2021). Counter-insurgency governance in the Sahel. International Affairs, 97(6), 1805–1823.
9. Döring, K. P. W. (2023). African military politics in the Sahel: Regional organizations and international politics. Cambridge University Press.
10. Economic Community of West African States. (2020). Priority action plan to eradicate terrorism in the ECOWAS region (2020–2024).
11. Economic Community of West African States. (2025). Experts meet in Abidjan to propose a regional action plan against illegal, unreported and unregulated fishing in West Africa.
12. ENACT. (2023). Africa organized crime index 2023.
13. European Civil Protection and Humanitarian Aid Operations. (2026). Democratic Republic of the Congo: Factsheet.
14. Global Centre for the Responsibility to Protect. (2026). Democratic Republic of the Congo: Country profile.
15. Global Initiative Against Transnational Organized Crime. (2023). Illicit economies and armed conflict in the Sahel: JNIM's financing model.
16. Gutierrez, E. D. (2020). The paradox of illicit economies: Survival, resilience, and the limits of development and drug policy orthodoxy. Globalizations, 17(6), 1008–1026.
17. ICC International Maritime Bureau. (2026). Piracy and armed robbery against ships: Report for the period 1 January–31 December 2025.

18. Idler, A. (2020). The logic of illicit flows in armed conflict: Explaining variation in violent non-state group interactions in Colombia. World Politics, 72(3), 335–376.
19. Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: At the crossroads of politics, sovereignty and cooperation. Policy Design and Practice, 6(2), 146–159.
20. Institute for Economics & Peace. (2024). Global terrorism index 2024: Measuring the impact of terrorism.
21. Institute for Economics & Peace. (2025). Global terrorism index 2025: Measuring the impact of terrorism.
22. Institute for Economics & Peace. (2026). Global terrorism index 2026: Measuring the impact of terrorism.
23. Internal Displacement Monitoring Centre. (2025). Global report on internal displacement 2025. INTERPOL. (2025). African cyberthreat assessment report 2025.
24. INTERPOL. (2026). African cyberthreat assessment report 2026.
25. Mensah, R. O. (2023). Experiences and perceptions of cybercrime victims in Ghana. Cogent Social Sciences, 9(2), 2285623.
26. Muggah, R. (2023). Organized crime in armed conflicts and other situations of violence.
27. International Review of the Red Cross, 105(923), 569–574.
28. Okul, J. O. (2026). Effectiveness of the maritime security architecture within the Western Indian Ocean region in addressing traditional, non-traditional and emerging threats. Frontiers in Political Science, 8, 1756401.
29. Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. The African Journal of Information and Communication, 28, 1–21.
30. Prah, A. (2023). Ad-hoc security initiatives in Africa: A new type of regional security arrangement. African Security, 16(4), 356–377.
31. Thurston, A. (2020). Jihadists of North Africa and the Sahel: Local politics and rebel groups.
32. Cambridge University Press.
33. United Nations Conference on Trade and Development. (2020). Economic development in Africa report 2020: Tackling illicit financial flows for sustainable development in Africa.
34. United Nations Conference on Trade and Development. (2024). Review of maritime transport 2024.
35. United Nations Conference on Trade and Development. (2025). Review of maritime transport 2025: Staying the course in turbulent waters.
36. United Nations Development Programme. (1994). Human development report 1994: New dimensions of human security.
37. United Nations Development Programme. (2023). Journey to extremism in Africa: Pathways to recruitment and disengagement.
38. United Nations Office for the Coordination of Humanitarian Affairs. (2026). Democratic Republic of the Congo humanitarian needs and response plan 2026.
39. United Nations Office on Drugs and Crime. (2020). Global study on firearms trafficking 2020. United Nations Office on Drugs and Crime. (2024). Global report on trafficking in persons 2024. United Nations Office on Drugs and Crime. (2025). World drug report 2025.
40. Vreÿ, F. (2020). Maritime security in Africa: Challenges and opportunities. In D. V. Malan (Ed.), Africa and the sustainable development goals (pp. 143–160). Springer.
41. Williams, P. D. (2021). Prospects for security in the Western Indian Ocean. Journal of the Indian Ocean Region, 17, 184–204.
42. World Bank. (2015). Withdrawal from correspondent banking: Where, why, and what to do about it.
43. World Bank. (2024). Mid-term review of the World Bank Group strategy for fragility, conflict, and violence (2020–2025).
44. World Bank Group. (2026). Democratic Republic of Congo: Country overview.
45. Zenn, J. (2020). Unmasking Boko Haram: Exploring global jihad in Nigeria. Lynne Rienner Publishers.
46. Zenn, J. (2021). Boko Haram's factional feuds: Internal extremism and external interventions.
47. Terrorism and Political Violence, 33(3), 616–648.