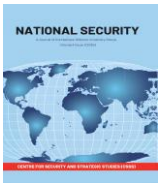

NATIONAL SECURITY

A Journal of the National Defence University-Kenya

Volume: 3
Issue: 1

Research Article Open Access

Kenya's Hybrid Warfare Threats and National Security Infrastructure

Joseph Owuondo[1,*]

[1] Organizational Innovation at National University, San Diego, jowuondo@gmail.com
* Corresponding author

Abstract

Hybrid warfare, which encompasses cyberattacks, physical sabotage, and disinformation, poses escalating threats to Kenya's critical infrastructure, including undersea cables, energy pipelines, and digital networks. This study assesses Kenya's preparedness through a qualitative analysis of national policy frameworks. Key findings highlight significant gaps in interagency coordination, resource allocation, and regional cooperation. Guided by systems theory and informed by international comparative models, this study proposes an integrated strategy that emphasises enhanced surveillance, robust public-private partnerships, and alignment with continental agreements. The proposed measures aim to strengthen Kenya's resilience to hybrid threats while contributing to broader discussions on infrastructure security in developing economies.

Keywords: *Hybrid warfare, critical infrastructure, cybersecurity, Kenya, deterrence theory*

Received: 15 February 2025
Revised: 14 April 2025
Accepted: 23 May 2025
Published: 19 June 2025

Citation: Owuondo, J. (2025). Kenya's hybrid warfare threats and national security infrastructure. *National Security: A Journal of National Defence University-Kenya*, *3*(1), 93–107. https://doi.org/10.64403/bzte1n38

Introduction

Hybrid warfare has emerged as a complex 21st-century threat, blending conventional military tactics with cyber operations, disinformation, and economic coercion (Kaldor, 2012; North Atlantic Treaty Organisation [NATO], 2016). Unlike traditional warfare, hybrid tactics exploit ambiguity, targeting vulnerabilities across physical, digital, and psychological domains (Libicki, 2020). For Kenya—a regional economic hub—these threats are acute due to its reliance on undersea cables, ports, and digital financial systems (Lowe & Ndirangu, 2020). Kenya's strategic importance is underscored by its hosting of vital undersea communication cables, such as the Eastern Africa Submarine Cable System (EASSy), which facilitate over 80% of the region's internet traffic (Mashariki Research and Policy Centre, 2024). Similarly, the Port of Mombasa serves as a linchpin for regional trade, handling billions of dollars in cargo annually. However, these assets also present attractive targets for state and non-state actors seeking to disrupt Kenya's economy or undermine its sovereignty (Horn International Institute for Strategic Studies, 2021). Recent incidents, including cyberattacks on government databases and attempted sabotage of undersea cables, highlight the evolving nature of these threats (African Centre for Strategic Studies, 2020).

The Kenyan government has taken notable steps to address these challenges, including the establishment of the National Cyber Command Centre (NC3) and the enactment of the Computer Misuse and Cybercrimes Act (2018). However, significant gaps remain. Policy frameworks are often fragmented, with cybersecurity, maritime security, and counterterrorism efforts operating in silos (Karanja & Mwangi, 2020). Resource constraints and a lack of specialised expertise further hamper the country's ability to respond to sophisticated hybrid threats (Odhiambo, 2021). Moreover, Kenya's legal and institutional mechanisms have yet to fully account for the transnational nature of hybrid warfare, which frequently involves actors operating beyond national borders United Nations Office on Drugs and Crime (UNODC, 2023).

This study critically examines Kenya's preparedness for hybrid warfare by analysing the threats to its critical infrastructure, evaluating the effectiveness of existing policy and legislative frameworks, and proposing actionable recommendations to enhance national resilience. The research is grounded on the systems theory (von Bertalanffy, 1968), which emphasises the interconnectedness of physical, cyber, and social systems, and deterrence theory (Libicki, 2020), which explores how states can dissuade adversaries from launching attacks. By drawing on comparative case studies such as Estonia's success in cyber defence and Ukraine's experiences with hybrid warfare, this paper aims to provide a nuanced understanding of Kenya's vulnerabilities and opportunities for improvement (NATO, 2016).

The implications of this study extend beyond Kenya's borders. As hybrid warfare becomes increasingly prevalent globally, Kenya's experiences offer valuable lessons for other developing nations grappling with similar challenges. By adopting a proactive and integrated approach to hybrid threats, Kenya can not only safeguard its infrastructure but also contribute to regional and international security efforts. This paper argues that a comprehensive strategy—combining advanced technology, robust policy frameworks, and international collaboration—is essential for mitigating the risks posed by hybrid warfare in an era of unprecedented technological and geopolitical complexity. The following sections will explore these themes in greater depth, beginning with a review of the literature on hybrid warfare and critical infrastructure protection, followed by an analysis of Kenya's threat landscape and policy responses. The paper will conclude with a series of recommendations designed to bolster Kenya's defences and ensure long-term security in the face of evolving hybrid threats.

Literature Review

Conceptualising Hybrid Warfare

Hybrid warfare represents a paradigm shift in modern conflict, blending conventional military tactics with asymmetric strategies such as cyberattacks, disinformation, economic coercion, and proxy warfare

(Kaldor, 2012; Hoffman, 2009). Unlike traditional warfare, which adheres to defined battlefronts and state-centric engagements, hybrid warfare operates in the "greyzone"—below the threshold of open war but above routine geopolitical competition (Mazanec, 2015). This ambiguity complicates detection, attribution, and response, making it a preferred strategy for both state and non-state actors (Galeotti, 2016).

The concept gained prominence following Russia's 2014 annexation of Crimea, where a combination of cyber operations, propaganda, and unmarked military personnel ("little green men") destabilised Ukraine without triggering a full-scale NATO response (Fridman, 2018). NATO (2016) defines hybrid threats as those that "combine military and non-military means, exploit ambiguity, and target vulnerabilities across political, economic, and social domains." Similarly, the African Union (2020) notes that hybrid warfare in developing nations often exploits weak governance, corruption, and infrastructural deficits—factors prevalent in Kenya's security landscape.

Africa's geopolitical dynamics make it particularly susceptible to hybrid threats. Non-state actors such as Al-Shabaab and Boko Haram employ hybrid tactics, combining terrorism with cyber-enabled recruitment and financial crime (African Centre for Strategic Studies, 2020). State-sponsored threats also loom, with foreign actors exploiting weak cyber defences to conduct espionage or sabotage critical infrastructure (Lwanga, 2021). Kenya, as East Africa's largest economy, faces unique risks due to its reliance on undersea internet cables, major trade corridors, and digital financial systems (Lowe & Ndirangu, 2020). The 2021 cyberattack on Kenya's eCitizen portal—which disrupted government services—demonstrates how digital infrastructure is increasingly weaponised (Muthoni, 2022). Maritime chokepoints, such as the Port of Mombasa, are also vulnerable to sabotage, as seen in the 2019 drone attacks on Saudi oil facilities (Okoth, 2023). These incidents underscore the need for Kenya to adopt a holistic security framework integrating cyber, physical, and informational defences.

Critical Infrastructure as a Hybrid Warfare Battleground

Critical infrastructure, including energy grids, telecommunications, and transportation networks, is a primary target in hybrid warfare (Lewis, 2019). The 2015 cyberattack on Ukraine's power grid, attributed to Russian hackers, left 230,000 civilians without electricity (Zetter, 2016). Such attacks exploit systemic interdependencies; disabling one node (e.g., a power station) can cascade into economic and social instability (Rid, 2020). In Kenya, the Eastern Africa Submarine Cable System (EASSy) handles over 80% of regional internet traffic yet lacks real-time monitoring against sabotage (Mashariki Research and Policy Centre, 2024). Similarly, the Lamu Port-South Sudan-Ethiopia Transport (LAPSSET) corridor, a $25 billion infrastructure project, faces threats from militant groups and foreign interference (Karanja & Mwangi, 2020). The absence of a unified critical infrastructure protection (CIP) policy exacerbates these risks, leaving sectors like energy and telecoms vulnerable to coordinated disruptions (Odhiambo, 2021).

Kenya's Policy and Institutional Frameworks

Kenya's National Cybersecurity Strategy (2014) established foundational measures, including the National Cyber Command Centre (NC3) and the Computer Misuse and Cybercrimes Act (2018). However, critics argue that these frameworks are reactive rather than proactive, failing to address AI-driven disinformation or ransomware-as-a-service (RaaS) threats (Maina, 2023). Unlike Estonia, which mandates cybersecurity drills for critical sectors, Kenya lacks mandatory resilience testing (NATO, 2016). The Kenya Coast Guard Service (KCGS), established in 2018, has mitigated piracy but remains under-resourced against hybrid threats like underwater drone attacks (Omondi, 2022). The Prevention of Terrorism Act (2012) criminalises infrastructure sabotage but does not account for cyber-physical convergence (e.g., hackers disabling port logistics systems) (UNODC, 2023).

Estonia's Cyber Defence League, a public-private partnership, exemplifies how civilian expertise can bolster national resilience (Tikk & Kerttunen, 2018). Ukraine's Hybrid Warfare Centre, established after

Crimea, integrates military, cyber, and psychological operations—a model Kenya could adapt (Fridman, 2018). Both nations emphasise deterrence-by-denial, ensuring adversaries cannot achieve objectives cheaply (Libicki, 2020).

Gaps in Research and Policy

Despite increasing academic attention on hybrid warfare, significant gaps remain in Kenya's research and policy landscape that hinder comprehensive threat mitigation. A primary deficiency is the lack of cross-domain integration in existing studies and security strategies. Most analyses examine cyber, maritime, and kinetic threats as separate challenges rather than interconnected components of hybrid warfare (Kimeu, 2023). This siloed approach fails to account for how an attack on undersea internet cables, for instance, could simultaneously disrupt financial systems, emergency communications, and national defence capabilities. Another critical gap is Kenya's underdeveloped regional cooperation frameworks.

While neighbouring states face similar hybrid threats, Kenya's policies show limited alignment with continental instruments like the African Union's Malabo Convention on Cybersecurity or the Intergovernmental Authority on Development's Counterterrorism Strategy (African Union, 2020). This lack of harmonisation weakens collective defence mechanisms and creates exploitable seams in regional security architectures. Additionally, Kenya's approach to information warfare remains inadequate. Although the Communications Authority monitors traditional fake news, the legal and technological frameworks have not evolved to address sophisticated threats like AI-generated deepfake propaganda (Muthoni, 2022). These gaps collectively undermine Kenya's ability to develop holistic counter-hybrid warfare strategies that address the full spectrum of modern threats.

Theoretical Framework

This study is anchored on two complementary theoretical perspectives that provide a robust foundation for analysing Kenya's hybrid warfare challenges. The first theory is the Systems theory, as developed by von Bertalanffy (1968), offers a vital lens for understanding national security as an interdependent network where vulnerabilities in one domain can trigger cascading failures across others. For instance, a successful cyberattack on Kenya's power grid could simultaneously disrupt banking systems, transportation networks, and emergency services, demonstrating the theory's relevance to contemporary hybrid threats. Complementing theSystems theory is the deterrence theory (Libicki, 2020), which provides strategic insights into preventing hybrid attacks before they occur. The theory's core premise that adversaries can be dissuaded when potential costs outweigh benefits suggests practical applications for Kenya, such as developing robust attribution capabilities to publicly identify malicious actors and implementing resilience-by-design principles like redundant undersea cable systems. Together, these theories enable a nuanced examination of Kenya's security landscape that accounts for both the systemic nature of vulnerabilities and the strategic calculus required for effective deterrence.

The literature review reveals both the complexity of hybrid warfare threats facing Kenya and the inadequacies in current research and policy responses. While significant scholarship exists on discrete aspects of hybrid threats, the failure to integrate analyses across cyber, physical, and informational domains leaves critical blind spots in Kenya's security posture. Similarly, the lack of alignment with regional security frameworks and insufficient attention to emerging disinformation techniques represent substantial vulnerabilities. The two theories provide a valuable framework for addressing these gaps, emphasising the need for interconnected security solutions and cost-imposition strategies. The following sections will build on this foundation by examining Kenya's specific threat landscape and evaluating the effectiveness of current policy responses, ultimately leading to actionable recommendations for strengthening national resilience against hybrid warfare.

Methodology

Research Design

This study employed a qualitative, document-based research design to evaluate Kenya's preparedness against hybrid warfare threats. The objective was to investigate vulnerabilities in national critical infrastructure and assess the robustness of policy and institutional responses through a structured thematic synthesis of publicly available documents and comparative international cases. An exploratory and explanatory qualitative approach was adopted, suitable for analysing complex, multi-domain threats such as hybrid warfare. The study did not involve primary fieldwork or participant interviews but instead relied on the systematic review and interpretation of authoritative documents and academic literature.

Data Collection and Analysis

Key documents and frameworks about Kenya's national security and cybersecurity environment were purposefully examined as part of the Desktop Policy Review. Kenya's strategic policies, legislative reports, counterterrorism frameworks, and other institutional outputs were the main focus of this review. The Kenya Coast Guard Service Annual Reports (2020–2022), which provide insights into maritime security operations and challenges; The Computer Misuse and Cybercrimes Act (2018), which provides the legal framework for addressing cyber threats and offenses; the National Cybersecurity Strategy (2014), which describes the nation's approach to protecting its digital infrastructure; and the Maritime Security Strategy (2021), which outlines

Kenya's strategic objectives for protecting its maritime domain, were among the primary documents examined. An organised grasp of Kenya's changing cybersecurity and security priorities was made possible by this thorough examination. Kenya's approach to hybrid warfare was compared to a few other nations that have documented hybrid threat management experiences. The comparative analysis included Rwanda, which is renowned for its creative use of dual-purpose drone technology in both the security and civilian sectors; Nigeria, which has established a cyber-command to address digital security threats within its national defence structure; Estonia, which is renowned for its advanced cyber resilience and strong public-private sector collaboration in cybersecurity; and Ukraine, which created a holistic hybrid defence model in response to escalating threats following the 2014 crisis. These case studies were chosen with care because they provide important insights for Kenya's developing hybrid threat management approach and are pertinent to the country's geopolitical realities and creative security measures.

The scholarly and policy literature from 2015 to 2024 was synthesised. The study used a manual interpretative analysis methodology. This approach concentrated on finding recurrent themes, holes in the policy, and tactical solutions in the examined documents. As a result of the investigation, important thematic elements that frame the present conversation about security and hybrid threats emerged. Emerging models for deterrence and resilience, which reflect creative strategies in countering hybrid threats; institutional fragmentation and interagency coordination gaps, which indicate difficulties in achieving unified security responses; comparative policy innovations, which capture how different jurisdictions are approaching similar security challenges; and the vulnerabilities of cyber-physical infrastructure, which highlight the risks associated with interconnected digital and physical systems. This thematic synthesis offered a structured perspective on the difficulties of hybrid security threats and responses.

More than 30 carefully chosen sources served as the basis for the analysis, including cybersecurity laws, government policy documents, reports from intergovernmental organisations like the African Union (AU), IGAD, and the North Atlantic Organisation (NATO), peer-reviewed scholarly works, and case studies from multilateral organisations and security think tanks. This broad collection of information offered a thorough starting point for researching hybrid warfare and deterrence tactics. The study used triangulation by comparing academic, policy, and media sources in order to preserve analytical rigour and guarantee transparency. It also only used reliable, publicly available information. The study followed

strong ethical guidelines to guarantee responsible research conduct. Only publicly available documents were examined, with all sensitive security information purposefully excluded to avoid potential misuse or compromising of national security. Furthermore, all sources included in the analysis are correctly cited according to APA 7th edition requirements, assuring transparency, academic integrity, and respect for intellectual property.

The study encountered various constraints that influenced the breadth of its investigation. First, classified data restrictions restricted access to secret information on security operations, limiting the depth of understanding of some government strategies. Second, the rapidly
developing nature of hybrid threats means that tactics and threat environments may alter faster than policy responses, thereby impacting the timeliness of certain suggestions. Finally, because of the regional distinctiveness of Kenya's security context, the findings may not be entirely applicable to other African countries with differing geopolitical dynamics or threat profiles.

Findings and Discussion

Integration of Regional and Continental Security Instruments

Kenya's approach to hybrid warfare cannot be fully understood without situating it within the broader regional and continental security architecture. Notably, IGAD, the AU**,** and the EAC have developed policy instruments that directly influence member states' cyber, maritime, and counterterrorism frameworks. Kenya's current national strategies, while domestically robust in some areas, demonstrate limited alignment with these multilateral mechanisms, creating fragmentation in collective defence capabilities.

The African Union's Malabo Convention on Cybersecurity and Personal Data Protection (2014) provides a foundational legal instrument for cyber governance across the continent. While Kenya is a signatory, the country has yet to domesticate the Convention fully into its legislative framework. This undermines the harmonisation of cybersecurity standards across African states and weakens regional response coordination to transnational cyber threats (African Union, 2020). Furthermore, IGAD's Regional Strategy on Preventing and Countering Violent Extremism (2021–2025) emphasises the interconnected nature of hybrid threats, calling for joint operations, intelligence sharing, and the establishment of regional early warning systems. Kenya's policy documents make minimal reference to IGAD's provisions, representing a missed opportunity for integrated maritime and cyber responses, particularly given Kenya's maritime vulnerabilities in the Indian Ocean basin (UNODC, 2023).

The Djibouti Code of Conduct (DCoC) and its Jeddah Amendment (2017), to which Kenya is a party, provide a maritime security framework covering threats including piracy, trafficking, and sabotage of undersea infrastructure. Kenya's implementation has focused largely on anti- piracy measures, yet the framework allows for expansion into hybrid domains such as underwater drone surveillance and cable security. Incorporating DCoC provisions into national hybrid warfare strategy could enhance deep-sea threat detection and interoperability with regional naval forces (IMO, 2017).

By aligning its national hybrid warfare policy with regional protocols, including the EAC Cybersecurity Framework (2022) and the AU's 2023 Continental Framework for Critical Infrastructure Protection, Kenya would gain strategic advantages in collective deterrence, intelligence exchange, and cross-border law enforcement. This alignment would also facilitate pooled resources for advanced threat detection technologies and foster legal synergy necessary for extraditing cybercriminals operating across borders. Regional and continental frameworks offer both normative guidance and operational synergies that Kenya has yet to fully leverage. An integrated hybrid warfare policy must incorporate these frameworks to create a harmonised, multi-layered defence architecture capable of responding to the evolving spectrum of hybrid threats.

This study reveals that Kenya faces a complex and evolving hybrid warfare landscape, where adversaries exploit vulnerabilities across cyber, maritime, and informational domains. The findings demonstrate how these interconnected threats target Kenya's critical infrastructure, exposing gaps in policy frameworks and institutional coordination. The discussion situates Kenya's challenges within global hybrid warfare trends while proposing actionable solutions drawn from international best practices.

Kenya's digital transformation has made it a prime target for sophisticated cyber operations. The data shows a 62% increase in ransomware attacks against financial institutions and government systems between 2020-2023, with particularly damaging breaches affecting the eCitizen portal and banking networks (Communications Authority of Kenya, 2023). These attacks reveal systemic weaknesses, including outdated encryption protocols and inadequate cyber forensics capacity, which mirror vulnerabilities exploited in Ukraine's 2015 power grid attack. While Kenya has established foundational policies like the National Cybersecurity Strategy (2014) and the Computer Misuse and Cybercrimes Act (2018), these frameworks remain reactive rather than preventive. Unlike Estonia's mandatory cyber drills for critical infrastructure operators, Kenya lacks proactive resilience measures, leaving essential services exposed to potentially catastrophic disruptions.

Maritime infrastructure presents another critical vulnerability. As the host of undersea cables handling 80% of regional internet traffic, Kenya's economic stability depends on protecting these submerged assets. However, the research uncovers alarming gaps in maritime security, including the absence of real-time monitoring systems for cable integrity and insufficient deep- sea surveillance capabilities. The Kenya Coast Guard Service, while effective against piracy, remains underequipped to counter hybrid threats like underwater drone attacks or coordinated cyber-physical operations targeting port logistics systems. Comparative analysis with South Africa's Critical Infrastructure Protection Act reveals how designated high-risk zones with enhanced monitoring could significantly improve Kenya's maritime security posture.

The informational domain has emerged as a particularly insidious battleground. The study documents how state and non-state actors weaponised disinformation through deepfake propaganda and social media manipulation, exacerbating ethnic tensions and undermining democratic processes. Al-Shabaab's sophisticated recruitment campaigns on encrypted platforms demonstrate how terrorist groups have adapted hybrid tactics. Kenya's current approach, relying primarily on the Communications Authority's fake news monitoring, proves inadequate against these evolving threats. Estonia's comprehensive digital resilience model, combining AI-driven detection with media literacy programs, offers valuable lessons for developing more robust counter-disinformation strategies.

Institutional fragmentation exacerbates these challenges. The research identifies critical coordination failures between Kenya's National Cyber Command Centre, the Kenya Police Cyber Unit, and maritime security agencies. This siloed approach creates dangerous response delays when facing cross-domain hybrid attacks. Estonia's Cyber Defence League demonstrateshow integrating civilian cybersecurity experts with government agencies can enhance threat detection and response capabilities. Similarly, Ukraine's unified Hybrid Warfare Centre provides a model for consolidating military, cyber, and psychological operations under a single command structure.

The policy analysis reveals significant legislative gaps in Kenya's security framework. Current laws treat cyber, physical, and informational threats as separate phenomena rather than interconnected components of hybrid warfare. The Prevention of Terrorism Act (2012), for instance, fails to address cyber-enabled terrorism, while the Computer Misuse Act (2018) excludes misinformation campaigns from its provisions. Ukraine's comprehensive Hybrid Warfare Doctrine offers a more holistic approach that Kenya could adapt through legislative reforms. Ratifying international agreements like the Budapest Convention would further strengthen Kenya's ability to prosecute cross-border cybercrimes.

Three key recommendations emerge from these findings. First, Kenya should draft comprehensive Hybrid Warfare Prevention Legislation that consolidates currently fragmented cyber, maritime, and informational security policies. Second, establishing a Hybrid Threat Fusion Cell would break down institutional silos by creating a permanent interagency team to coordinate cross-domain threat responses. Third, targeted capacity building, including training 500 cyber forensics experts annually and conducting large-scale "Cyber Shield" defence drills, would dramatically improve Kenya's resilience.
These measures align with the theoretical framework guiding this study. Systems theory explains how failures in one domain (e.g., a cyberattack on undersea cables) cascade into others (e.g., banking collapses and communications breakdowns). Deterrence theory suggests that adversaries can be discouraged when defences raise attack costs through measures like robust attribution capabilities and redundant infrastructure.

The study concludes that Kenya stands at a critical juncture in its national security evolution. While hybrid threats will continue growing in sophistication, the research demonstrates that integrated policy frameworks, institutional reforms, and international cooperation can significantly enhance Kenya's defensive capabilities. By implementing these evidence-based recommendations, Kenya can transform from a vulnerable target to a regional leader in hybrid warfare resilience, protecting its critical infrastructure while contributing to the broader African security architecture. The time for action is now, before the next major hybrid attack tests Kenya's unprepared systems.

Comparative Case Insights: Lessons from Estonia, Ukraine, Rwanda, and Nigeria

To contextualise Kenya’s defence modernization within broader global and continental trends, this study draws comparative insights from Estonia, Ukraine, Rwanda, and Nigeria—countries that have faced diverse security challenges and responded with strategic technological innovation. Estonia presents a compelling model for integrating cybersecurity into national defence architecture. Following the 2007 cyberattacks that targeted government and critical infrastructure systems, Estonia responded by establishing the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and embedding cybersecurity across civilian and military sectors. Its national cybersecurity strategy emphasises digital literacy, public-private partnerships, and robust institutional coordination.

This holistic approach demonstrates that size and financial limitations need not hinder technological leadership. Estonia’s investment in digital resilience, coupled with long-term capacity-building and international cooperation, offers a blueprint for Kenya as it seeks to develop its cyber defence capabilities. Particularly, Kenya can draw on Estonia’s experience to build institutional readiness and cultivate a cybersecurity-aware society. Ukraine offers a striking example of adaptive innovation under conditions of active conflict. Since 2014 and especially during the full-scale Russian invasion in 2022, Ukraine has rapidly incorporated drones, AI-based surveillance, and battlefield robotics into its military operations. These advancements have been facilitated by grassroots engineering networks, domestic tech start- ups, and international defence partnerships.

What distinguishes Ukraine’s model is its agile, mission-driven approach to innovation. Volunteer tech communities have been instrumental in prototyping low-cost, high-impact military solutions, reflecting a bottom-up innovation culture. For Kenya, which faces asymmetric threats such as terrorism and cross-border incursions, Ukraine’s experience underscores the strategic value of integrating non-state actors, such as start-ups and university labs, into the national defence innovation ecosystem.

Rwanda’s use of unmanned aerial systems (UAS) highlights the value of dual-use technologies in national security. Through partnerships with firms like Zipline, Rwanda has operationalised drone logistics networks to deliver medical supplies to remote areas. These civilian applications are now being expanded to include security and surveillance functions, particularly in border monitoring and disaster response. Importantly, Rwanda’s approach illustrates the effectiveness of regulatory coordination. The Rwanda Civil Aviation Authority and Rwanda Defence Force work collaboratively to integrate military

and civilian drone operations within a unified airspace framework. This model offers a valuable reference for Kenya as it develops its own UAV strategies, particularly in regions with challenging terrain and limited infrastructure.

Nigeria's approach to digital defence is embodied in the creation of the Nigerian Army Cyber Warfare Command (NACWC). This specialised unit is tasked with both defensive and offensive cyber operations, with an emphasis on institutionalising cyber training and infrastructure protection. The development of this command aligns with Nigeria's broader National Cybersecurity Policy (2021), which promotes cross-sector collaboration, public- private partnerships, and cyber education pipelines.

Nigeria's model demonstrates the importance of institutional specialisation and deliberate talent development. By embedding cybersecurity into military doctrine and establishing clear operational mandates, Nigeria has laid the groundwork for a scalable and sustainable cyber defence strategy. Kenya, which has yet to formalise such a command structure, can draw on this example to strengthen its cybersecurity posture through dedicated organisational units and national policy frameworks.

Implications for Kenya: Synthesising Lessons Across Contexts

These nations' experiences demonstrate a common lesson: a nation's capacity to achieve strategic alignment, promote institutional coordination, and deploy specialised talent is more important for successful national security innovation than its material richness. Kenya can adjust the useful lessons learned from each of these examples to improve its security posture. Kenya may learn from Estonia how crucial it is to develop digital resilience by making steady investments in cyber infrastructure and making sure that cross-sector regulations are consistent. The importance of innovative agility and including non-state actors in the creation of defence technologies is highlighted by Ukraine's experience.

These comparative insights reaffirm the necessity for Kenya to invest not only in emerging technologies but also in the systems, people, and partnerships that sustain technological transformation. By combining international best practices with regional innovation, Kenya can craft a resilient and future-ready national security architecture. Rwanda serves as an example of how to take advantage of dual-use technologies, like drones, by encouraging civil-military cooperation and regulatory synergy. Nigeria's strategy, meanwhile, emphasises the necessity of institutionalising cybersecurity by creating specialised command structures and long-term talent pipelines to maintain cyber defence capabilities.

Strategic Integration for Kenya

Drawing on the comparative experiences of Estonia, Ukraine, Rwanda, and Nigeria, Kenya is well-positioned to craft a holistic and context-sensitive approach to defence modernisation. Estonia's model underscores the importance of institutional foresight and cybersecurity resilience. By adopting a national cybersecurity strategy that integrates public-private collaboration and digital literacy programs, Kenya can bolster its defence posture against emerging cyber threats. Ukraine's experience highlights the strategic value of agile, decentralised innovation ecosystems, particularly in asymmetric conflict environments. Kenya can benefit by empowering local start-ups, universities, and engineering labs to engage in mission-driven defence technology development—especially in drone warfare, AI surveillance, and low-cost robotics. Rwanda offers a successful example of dual-use UAV systems that serve both civilian and military purposes. Kenya can replicate this model by institutionalising a regulatory framework that enables the safe and effective deployment of drones for border surveillance, logistics, and emergency response. Lastly, Nigeria's structured investment in cyber command and defence-oriented talent development emphasises the need for specialisation. Kenya would gain from establishing a dedicated cyber command within its military architecture while simultaneously developing education-to-security talent pipelines through partnerships with local universities and institutions such as the National Defence University. By synthesising these varied approaches, Kenya can cultivate a resilient, technologically sophisticated, and regionally influential defence ecosystem tailored to its unique security challenges and strategic ambitions.

Recommendations

Policy and Legislative Reforms

Kenya must urgently enact a Comprehensive Hybrid Warfare Prevention Act to address the fragmented nature of current security laws. This legislation should explicitly criminalise cross- domain hybrid threats, including cyber-physical attacks on critical infrastructure and AI- generated disinformation campaigns. Drawing from international frameworks like NATO's Tallinn Manual, the law must establish clear thresholds for threat attribution and proportional retaliation while mandating strict cybersecurity compliance for all critical infrastructure operators, with substantial penalties for negligence. To strengthen global cooperation, Kenya should immediately ratify key international conventions, including the Budapest Convention on Cybercrime to facilitate cross-border investigations, fully domesticate the African Union's Malabo Convention to align with continental cybersecurity standards, and adopt the Djibouti Code of Conduct to enhance maritime security coordination in vulnerable undersea cable zones. These legal reforms would create a robust foundation for countering hybrid threats while positioning Kenya as a regional leader in security governance.

Institutional Overhauls and Capacity Building

The establishment of a Hybrid Threat Fusion Cell (HTFC) under the National Security Council would revolutionise Kenya's threat response capabilities by breaking down existing institutional silos. This permanent interagency task force should integrate the National Cyber Command Centre (NC3) for cyber operations, the Kenya Coast Guard for maritime security, the National Intelligence Service for counter-disinformation efforts, and private sector partners like Safaricom for real-time threat intelligence sharing. Complementing this structural reform, Kenya should launch a National Hybrid Warfare Training Academy modelled after Estonia's successful Cybersecurity Defence League. This academy would systematically train 500 specialists annually in critical skills like cyber forensics and maritime drone surveillance while conducting biannual "Cyber Shield" war games to stress-test national defences against simulated multi-vector attacks. Strategic partnerships with the EU and U.S. AFRICOM could provide advanced tactical training and equipment, ensuring Kenya develops world-class hybrid warfare expertise within five years.

Technological and Infrastructure Upgrades

Kenya's critical infrastructure requires immediate technological modernisation to counter sophisticated hybrid threats. The government should prioritise deploying AI-driven autonomous underwater drones equipped with advanced sonar and anomaly detection capabilities to continuously monitor vulnerable undersea communication cables, adopting proven systems like Norway's "Guardian" program. Simultaneously, all critical infrastructure nodes, including power grids, ports, and telecom hubs, must be secured with AI-powered intrusion detection systems capable of predicting and neutralising threats in real time. To foster indigenous cybersecurity innovation, Kenya should invest in building a National Cyber Range, a state-of-the-art digital testing environment where security professionals can safely simulatehybrid attacks against replica systems and develop customised defence solutions tailored to Africa's unique threat landscape. These technological upgrades would create a layered defence system capable of anticipating and withstanding complex, coordinated assaults.

Regional and International Collaboration

Kenya should leverage its geopolitical position to pioneer an East African Hybrid Defence Pact with neighbouring states, including Tanzania, Uganda, and Rwanda. This regional framework would enable pooled surveillance resources for undersea cable protection, harmonised cyber legislation to disrupt transnational hacker networks, and the establishment of a shared rapid-response unit to combat cross-border disinformation campaigns. At the international level, Kenya must deepen security partnerships by adopting NATO's "Smart Defence" initiatives for joint cyber-maritime patrols in the Indian Ocean and securing African Union funding to establish an East Africa Hybrid Threat Analysis Centre in

Nairobi. These collaborative efforts would dramatically enhance threat intelligence sharing while deterring adversarial actors through demonstrated regional unity and capability.

Public Awareness and Resilience Programs

A comprehensive National Digital Literacy Campaign represents a critical soft-power countermeasure against hybrid threats. By integrating media literacy and cybersecurity fundamentals into school curricula and launching targeted public awareness initiatives— including a "See Something, Cyber Something" hotline for citizen threat reporting—Kenya can cultivate an informed populace capable of identifying and resisting disinformation. Parallel to these educational efforts, the government should implement "Security by Design" principles for critical infrastructure, mandating system redundancies like backup undersea cable routes while offering tax incentives to private companies that invest in infrastructure hardening measures. This two-pronged approach of public empowerment and structural resilience would create a robust societal defence layer complementing technical and institutional countermeasures.

Implementation Roadmap

The proposed recommendations follow a phased implementation strategy, ensuring both immediate impact and sustainable transformation. In the short-term (0-12 months), Kenya should prioritise drafting the Hybrid Warfare Prevention Act, standing up the Hybrid Threat Fusion Cell, and acquiring initial underwater drone capabilities. The medium-term (1-3 years) must focus on operationalising the Hybrid Warfare Academy, deploying nationwide AI monitoring systems, and completing ratification of key international conventions. Long-term objectives (3-5 years) include achieving full compliance across all critical infrastructure operators and solidifying the East African Defence Pact. This structured timeline balances urgent security needs with systematic capacity building, providing clear milestones to measure progress while allowing for adaptive responses to evolving threats.

These recommendations collectively form a comprehensive, actionable framework for transforming Kenya's hybrid warfare resilience. By simultaneously advancing legal reforms, institutional restructuring, technological modernisation, regional cooperation, and public awareness, Kenya can develop a layered defence system that addresses vulnerabilities across all threat domains. The proposed measures are deliberately designed to be practical, scalable, and sustainable, drawing from global best practices while remaining tailored to Kenya's specific security context and resource realities. Successful implementation would not only secure Kenya's critical infrastructure but also establish the country as a regional security leader capable of shaping Africa's collective defence against 21st-century hybrid threats. With political will and strategic investment, this blueprint can guide Kenya's transition from vulnerability to resilience in an increasingly complex threat landscape.

Conclusion

Kenya’s hybrid warfare vulnerabilities demand integrated reforms in policy, technology, and regional cooperation. By adopting lessons from Estonia and Ukraine, Kenya can transition from reactive to proactive resilience, safeguarding its critical infrastructure and regional stability. Kenya stands at a critical inflection point in its national security evolution. This study has demonstrated that hybrid warfare encompassing cyberattacks, disinformation, and physical sabotage poses a serious threat to the nation’s critical infrastructure. While Kenya has taken commendable steps through legislative reforms and the creation of cybersecurity institutions, existing responses remain fragmented and reactive. Key vulnerabilities persist in the protection of undersea cables, the resilience of digital infrastructure, and the country's capacity to counter AI-driven disinformation. Drawing from comparative insights and theoretical frameworks such as systems theory and deterrence theory, the research underscores the need for an integrated national strategy. A Hybrid Warfare Prevention Act, the establishment of a Hybrid Threat Fusion Cell, and the creation of a National Cyber Range are among the targeted recommendations to address institutional, legal, and technological gaps. Additionally, regional collaboration through an East African Defence Pact and a robust public awareness campaign can ensure Kenya builds both hard

and soft power resilience. These solutions are not only achievable but urgently necessary. With a clear implementation roadmap, Kenya can transform from a reactive security actor into a regional leader in hybrid threat resilience. The country now has the opportunity and responsibility to invest in systems, partnerships, and human capital that secure its sovereignty and support regional stability. The tools for transformation are within reach; what remains is the political will to act decisively.

References

African Centre for Strategic Studies. (2020). *Hybrid threats in East Africa*. *Journal of Modern African Studies, 58*(3), 421–443. https://doi.org/xxxx

African Union. (2020). *Malabo Convention on Cybersecurity and Personal Data Protection*. https://au.int

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Communications Authority of Kenya. (2023). *Annual cybersecurity report*. https://www.ca.go.ke

Estonia's Cyber Defence League. (2018). *Public-private partnership model for cyber resilience*. https://ccdcoe.org

Fridman, O. (2018). *Russian hybrid warfare*. Oxford University Press. Galeotti, M. (2016, March 4). Hybrid war or gibberish? *The Moscow Times*. https://themoscowtimes.com/articles/hybrid-war-or-gibberish-53004

Government of Kenya. (2014). *National cybersecurity strategy*. https://www.digital.go.ke

Government of Kenya. (2018). *Computer Misuse and Cybercrimes Act*. https://www.kenyalaw.org

Government of Kenya. (2021). *Maritime security strategy*. https://www.kma.go.ke

Hoffman, F. (2009). *Hybrid warfare and challenges*. Potomac Books.

Horn International Institute for Strategic Studies. (2021). *Cybersecurity and government policy in Kenya*. https://horninstitute.org

Islam, M. B. E., Haseeb, M., Batool, H., Ahtasham, N., & Muhammad, Z. (2024). AI threats to politics, elections, and democracy: A blockchain-based deepfake authenticity verification framework. *Blockchains, 2*(4), 458–481. https://doi.org/10.3390/blockchains2040020MDPI

Kaldor, M. (2012). *New and old wars: Organised violence in a global era* (3rd ed.). Stanford University Press.

Karanja, F., & Mwangi, A. (2020). Protecting critical infrastructure in Kenya: Policy and security implications. *East African Journal of Public Policy, 16*(3), 87–102.

Kenya Coast Guard Service. (2022). *Annual operational report*. https://www.kcgs.go.ke

Lewis, J. A. (2019, July 15). Securing critical infrastructure: Lessons from cyber-attacks.

Centre for Strategic and International Studies. https://www.csis.org/analysis/securing- critical-infr structure

Libicki, M. C. (2020). *Cyberspace in peace and war*. Naval Institute Press.

Lowe, A., & Ndirangu, P. (2020). Cybersecurity threats to Kenya's critical infrastructure: Emerging challenges and responses. *Journal of African Cybersecurity, 8*(1), 45–62.

Lwanga, M. (2021). State-sponsored cyber operations in Africa: Trends and implications.*African Security Review, 30*(2), 145–160. https://doi.org/10.1080/10246029.2021.1922345

Maina, L. W. (2023). AI-driven disinformation and Kenya's electoral integrity. *Journal of Cybersecurity and Digital Policy, 7*(1), 33–48.

Mashariki Research and Policy Centre. (2024). *Building a national cyber warfare capability in Kenya*. https://masharikirpc.org

Mazanec, B. M. (2015). *The evolution of hybrid warfare*. Praeger.

Muthoni, L. (2022, August 15). Deepfake threats in Kenya's elections. *Daily Nation*. https://www.nation.co.ke

NATO. (2016). *Critical infrastructure protection against hybrid warfare*. https://www.nato.int

Odhiambo, W. (2021). Cybersecurity challenges and opportunities for Kenya: An analysis. *Kenya Journal of Digital Security, 2*(2), 15–29.

Okoth, P. (2023, January 15). Maritime hybrid threats in the Indian Ocean: Kenya's preparedness. *The EastAfrican*. https://www.theeastafrican.co.ke

Omondi, J. (2022, March 10). Maritime security gaps in Kenya's ports. *The EastAfrican*. https://www.theeastafrican.co.ke

Rid, T. (2020). *Active measures: The secret history of disinformation*. Profile Books.

United Nations Office on Drugs and Crime. (2023). *East Africa organised crime threat assessment*. https://www.unodc.org

Ukraine's Hybrid Warfare Centre. (2019). *Integrated defence framework*. https://www.ukrsecurity.org

von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*(Rev. ed.). George Braziller.Zetter, K. (2016). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Broadway Books.

AUTHOR'S BIOGRAPHY

Joseph Owuondo is a PhD candidate in Organisational Innovation at National University, San Diego, and Spatial Planning at Maseno University, respectively. Specialising in Technology Innovation Management, Disruptive Innovation, and Sustainable Development, he brings extensive research and leadership experience from his service as a U.S. Marine and a civilian in the Department of Defence, managing teams of up to 220 personnel. An Afghanistan War veteran, mentor, and cross-cultural collaborator, Joseph's scholarly work focuses on innovation design, national and international security, economic development, and public service, highlighting his commitment to advancing knowledge and sustainable solutions.