NATIONAL SECURITY

A Journal of the National Defence University-Kenya

Volume: 3
Issue: 2

Research Article Open Acces

From Guns to Governance: Rethinking Responses to Hybrid Security Threats Beyond the Battlefield: Global, Regional and Kenyan Perspectives

Raphael Muthama Kapemba[1] *,

[1] African Nazarene University- rkapemba62526@anu.ac.ke

* Corresponding author

Abstract

Do governance-focused solutions supplement military activities in the successful management of hybrid security threats outside the battlefield in Kenya, as well as within international and regional approaches? The 21st century has witnessed a paradigm shift in war strategies, where the conventional approach to warfare through the military is no longer applicable, but rather through asymmetrical warfare that defies borders. Almost all non-state actors have evolved to become more complex, dynamic, uncertain and sophisticated, employing a combination of conventional, irregular and kinetic tactics. Such hybrid types of insecurity, including terrorism, cybercrime, climate-related insecurity, organised transnational crime and disinformation campaigns, reveal the shortcomings of solely military actions. This paper proposes that a governance-based approach, with an emphasis on institutional legitimacy, human security, socio-economic resilience and inclusive governance, is the required path forward to supplement traditional brutal power tactics by shifting the focus away from guns, which can endanger the stability of the state, security and sustainability. This paper examines hybrid threat factors in the global, regional and Kenyan contexts, drawing on the Human Security Theory, through qualitative desktop research that utilises academic articles, policy reports and global reports. The paper confirms that the best responses to hybrid warfare are balanced, striking a balance between the use of force and governance through the capacity of the security sector, as well as the reform of governance, community involvement and empowerment. The results highlight the role of the Human Security paradigm in diagnosing and responding to hybrid threats in Kenya, where governance failures are actively exploited.

Keywords: *Governance, Hybrid security threats, Human Security Theory, Human Security, Securitisation.*

Received: 20 May 2025
Revised: 23 August 2025
Accepted: 27 October 2025
Published: 15 December 2025

Citation: Kapemba, R. M., (2025). From Guns to Governance: Rethinking Responses to Hybrid Security Threats Beyond the Battlefield: Global, Regional and Kenyan Perspectives. *National Security: A Journal of National Defence University-Kenya*, *3*(1), 84–97.

DOI:

https://doi.org/10.64403/n26w7d18

Introduction

The 21st century has seen an increase in myriad global security threats, encompassing conventional and hybrid threats, as well as unconventional warfare characterised by its military, political, economic and cyber aspects (Hoffman, 2007). This realisation contradicts the classical belief that only military power can result in national security. The paper will contribute to the literature by critically analysing the effectiveness of governance-centred solutions in countering hybrid threats in Kenya, as well as the insights provided by international and regional (African) perspectives. Although it is argued that force modernisation is critical to national defence and the state of governance, some claim that the foundation of sustainable security lies in the strength of the governance, institutional legitimacy and trust in the government, thus creating the traditional divide between the hard-power and governance-based strategies (Rotberg, 2004; Luckham & Kirk, 2013). Securitisation theory and Human Security Theory are beneficial in framing this tension. The former tells us of the way in which problems are described and become existential threats that require extraordinary means. In contrast, the latter focuses on the freedom of individuals to be unafraid, to want and to be indignant. Collectively, these frames make sense of why excessive use of force may lead to the increase of insecurity and why governance-focused de-securitising policies can create resilient societies.

Hybrid threats have become a complicated phenomenon that is not confined to the conventional battlefield on the global scene. During the Cold War, the focus was on a single adversary: The Soviet Union. The distinction between war and peace was more apparent and given. Nations could agree and fight a common enemy using specific military strategies. Bachmann, Putter and Duczynski (2023) argue that, as the distinction between state and non-state actors is declining, the world is confronted with various threats from both state and non-state actors across all domains, including land, sea, air, space and cyberspace. The enemy in today's world is challenging us not just with bombs and aircraft but also with bots and algorithms. In this unpredictable world, more brutal terrorist groups like ISIS (Islamic State of Iraq and Syria) and more sophisticated cyber-attacks are being witnessed. China's rise as a superpower is also increasing geopolitical competition. The Russian invasions of Crimea (2014), ISIS in the Middle East and encroachment into Western elections of cyber interference demonstrate how governance vulnerabilities and societal divisions are exploited by non-state and state actors (Renz, 2016). For this purpose, global institutions such as the United Nations and the North Atlantic Treaty Organisation (NATO) have begun re-evaluating security frameworks in terms of resilience, institutional governance capacity and social cohesion as the first lines of defence (NATO, 2020).

The BANI framework, which stands for Brittle, Anxious, Nonlinear, and Incomprehensible, was introduced by Cascio to highlight the new characteristics of the world systems that are already very fragile, psychologically destabilizing, unpredictably complex, and cognitively overwhelming. It is not a replica of the VUCA model but offers different aspects of the same reality. BANI points at the hidden fragility of adopting an absolute strong institution belief (brittle), the widespread societal anxiety caused by uncertainty (anxious), the unpredictable and cascading nature of cause-and-effect relationships (nonlinear), and the increasing inability to make sense of the world that is full of data and rapid changes and during which one has to keep on learning and unlearning (incomprehensible). Notably, the framework serves as a conceptual tool for understanding systemic risk and facilitates the emergence of resilience-focused governance and adaptive leadership strategies in the era of accelerating disruption (Cascio, 2020).

Hybrid threats were finding a soft target on the African continent, due to a lack of governance, economic insecurity and low institutional capacity. The Sahel has turned out to be a playground of extremism and transnational organised crime and cyber threats continue destroying the national sovereignty (Aning & Atta-Asamoah, 2011). Military interventions, previously as unavoidable as they may seem, have failed to deliver long-term peace without governance reforms and citizen participation. This is the case with the Somali experience, which has, over the years, involved numerous actors in its quest for peace, among them the African Union (AU)/African Union Mission in Somalia (AMISOM), which has recently been transformed into the African Union Transition in Somalia (ATMIS). In certain areas, it was maintained by force, which gave only temporary stability, as it was not very strong because of other reasons that included poverty, unemployment and a lack of national unity.

Williams et al. (2018) noted that military use would not be enough to create any sustainable peace in Somalia, but development would only be manifested when governance, dialogue and reconciliation are strengthened with security operations. The appropriate example to illustrate this is Kenya, which has been had to deal with terrorism, cybercrime, violent extremism and electoral disinformation, all of which have underscored the inefficiency of the hard-power responses (Botha, 2014). The Al-Shabaab raids in the North Eastern part of Kenya, in particular, have demonstrated that the causes of insecurity have not only to do with governance collapse, corruption and socio-economic marginalisation but also with foreign threat. The militia gang has managed to infiltrate the Kenyan intelligence. It has continuously targeted our security agencies in very unpredictable attacks, not to mention that it has also threatened the economy of our nation by instilling fear among the locals and even potential investors (International Crisis Group, 2018). The town of Lamu, which was once the centre of tourism, has, in the last ten or so years, turned into a war zone as far as the gang activities are concerned, with an abundance of military force being deployed to instil more fear than peace. Therefore, the appeal to change guns to governance is the global-to-local reconsideration of how the concept of security should be interpreted and implemented.

This paper sought to establish how governance-based approaches can complement military tactics in addressing hybrid threats. It argues that the integration of good governance, institutional legitimacy and socio-economic empowerment enhances long-term resilience in security architecture. In the end, it demonstrates that the future of security is not only in the hands of military power, but also in the states' ability to govern and the faith of their citizens, thereby achieving the goal of shifting from the traditional combat approach of the military to governance-based approaches.

Theoretical Framework

Human Security Theory

This article applies the Human Security Theory (HST) in an effort to recast security from the traditional protectionist view of the state to one that prioritises the empowerment and protection of individuals. It emphasises freedom from fear, want and indignity, ideals that together constitute the pillars of societal resilience. According to the 1994 United Nations Human Development Report, the HST conceptualises security from a multidimensional perspective, encompassing dimensions such as economic, food, health, environmental, personal, community and political domains. Precisely, this holistic theory was well-suited for addressing the core research question that interrogated the capability of governance-centred approaches in complementing military efforts towards addressing hybrid security threats. To effectively address the challenge of operationalisation, this study employs an analytical framework that links key human security dimensions to hybrid threats through specific indicators.

The applicability of HST to this study is underscored by its emphasis on addressing the underlying vulnerabilities that hybrid actors exploit. Empirical studies have shown that grievances related to horizontal inequalities (Stewart, 2008) and the "youth bulge" phenomenon, when combined with limited economic opportunities, create fertile ground for recruitment by violent extremist groups and other hybrid threats (Omeje, 2013; Botha, 2014). With these drivers of structural change at the centre stage, HST offers a sound platform where governance reforms, inclusive development and community resilience can be regarded as a precautionary security measure.

Table 1

Analytical Framework: Human Security Dimensions and Hybrid Threats

Dimension	Linkage to Hybrid Threats	Indicator
Economic Security	Poverty and unemployment create grievances that are exploited for recruitment into criminal or extremist groups.	Youth unemployment rates, poverty indices and perceived economic marginalisation in certain regions.
Political Security	Political exclusion and corruption erode state legitimacy, thereby perpetuating support for anti-government elements.	Levels of public trust in institutions, perceptions of corruption and inclusivity in political processes.
Community Security	Where there is inter-communal strife and weak social cohesion, hybrid actors find opportunities to create division and rally supporters.	Past conflict between ethnic or religious groups, the degree of social trust and the existence of mechanisms for conflict resolution at the community level.
Personal Security	Direct physical violence from terrorism, organised crime and police brutality.	Incidence of terrorist attacks, crime rates and reports of human rights abuses by security forces.

Source: Researcher (2025)

Critiques of HST believe that its conceptual generosity renders it analytically vague and inappropriate for translation into policy and research (Paris, 2001; MacFarlane & Khong, 2006). According to the practitioners, this fuzziness presents a challenge in countries such as Kenya, where counterterrorism policy requires priorities that are clear and implementable. For example, a framework that categorises nearly everything as a social deficit and a security risk might make resource distribution difficult and create ambiguity about which institutions should lead specific interventions. However, on their part, the advocates of HST counter that this very breadth is what makes the theory applicable in situations where, instead of violent extremism and youth radicalisation, we have climate-related displacement (Newman, 2010; Tadjbakhsh & Chenoy, 2007). Rather than limiting policy to militarised reactions, Human Security provides a more flexible and integrative approach that assists Kenyan agencies not only in responding to symptoms of insecurity but also in addressing the structural causes of the same, as seen in the multi-agency findings and recommendations of this paper.

Integrated Theoretical Perspective

Although HST is the primary theory used to diagnose vulnerability, this paper incorporates the Securitisation theory to understand state reactions. The joint framework assumes that the origins of the hybrid threats lie in the lack of human security. However, the proper instruments of counter-strategy may be a de-securitisation of the challenges, which pushes the challenges outside the boundary of emergency military response and within the framework of regular political processes, including governance, dialogue and development. The combination of such a theory helps answer the question of why a purely militarised response (securitised) is indeed counterproductive and why truly sustainable resilience is not. In Kenya, an example of how the principles of human security can be translated into community-level education and economic interventions is the National Strategy to Counter Violent Extremism (NSCVE, 2016), which describes how a general framework can be transformed into specific policy tools. Therefore, although this is one of the concepts that still requires specification in research and policy-making, clear operational indicators, measurable targets and

monitoring systems are, in turn, inherently beneficial as a normative and practical conceptual framework through which hybrid threat responses can be viewed.

Stated differently, HST shifts the interrogative angle from who poses a threat to the state to what poses a threat to the people. It also indicates that evidence suggests resilient, inclusive societies are those that offer sustainable peace, as opposed to militarised reactions. This theoretical perspective, combined with securitisation theory, is directly reflected in the study's recommendations for governance reforms, livelihood improvement and participatory security strategies.

Methodology

This paper employs a qualitative research methodology, utilising a desktop study to examine previous literature on the topic of study. Due to the limitations inherent in primary data collection, the current research was restructured as a systematic critical review, following the principles of PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) to ensure a transparent and reproducible selection process. Several academic databases, including JSTOR, Google Scholar, Scite.ai, Research Rabbit and specialised repositories such as the Institute of Security Studies (ISS) and the International Crisis Group (ICG), were searched. A systematic set of keywords was developed, which meets the study aims, among them are such words as "hybrid threats," "human security," "Securitisation," and "Governance," which were included in the search to make sure that the new developments are detected and relevance is also achieved. Peer-reviewed journal articles, academic books, policy papers, official reports and conference proceedings that directly addressed the research themes were the inclusion criteria. Exclusion criteria also included the sources not being written in English, not being published during the period of time and not writing about the subject matter substantially or in a theoretical manner. Preliminary eligibility was done using titles and abstracts and full texts were assessed using pre-identified criteria.

The data were deciphered and aimed at the main points, methodologies, conclusions and theories. Data analysis was conducted with the help of thematic analysis, which is quite a standard practice in qualitative research to identify, analyse and interpret the patterns and themes that are presented in the text (Nowell et al., 2017). This process involved the familiarisation with data, generation of themes and summary of the key findings, which are consistent with the existing models of rigorous and transparent qualitative analysis. The thematic analysis method was well planned to give clear data analysis. The literature was treated with special attention, with counterarguments, criticism and alternative interpretations being included, which is one of the ways to prevent confirmation bias and come up with a strong and credible analysis.

Hybrid Warfare and Conceptualisation of Governance Responses

Since its introduction, hybrid warfare has had different interpretations, giving it the implication that it does not have a clear definition. As Hoffman (2007) explains, the term hybrid warfare can be used to refer to the employment of conventional weaponry, irregular warfare, terrorism and criminality within a time and space to meet a political goal. In the more recent definition, scholars have added such aspects of hybrid strategies as cyber operations, information warfare and economic manipulation (Goncalves, 2020). The constantly expanding definition is evidence of the fact that hybrid warfare cannot be considered fixed, but rather it is constantly developing in accordance with changes in technology, politics and social life. This paper identifies hybrid threats as multi-domain phenomena that can only be mitigated through an integrated military and governance response, along with societal responses. The following working definitions and typology are established to clarify the central concepts of this paper:

Hybrid threats are a state and/or non-state adversary's directed combination of conventional, irregular, cyber and criminal tools to achieve strategic objectives while remaining below the threshold of formal war.

Governance-centred approaches are those that address strengthening institutional legitimacy, accountability and transparency; ensuring inclusive political participation; protecting civil liberties; and addressing socio-economic drivers of instability through the delivery of public services and equitable development.

"Guns" vs. "Governance" Typology

"Guns": For this study, the term applies to traditional security approaches, including military strikes, kinetic counterterrorism operations, border militarisation, intelligence-led arrests and special forces deployments.

"Governance": In this article, it refers to the soft security approaches, such as anti-corruption reforms, judicial independence, community policing, youth employment programs, civic education, investment in social services and inter-agency coordination on Preventing and Countering Violent Extremism (P/CVE).

Discussion and Findings

Global Dimensions of Hybrid Warfare

Hybrid threats are manifested globally as indicators of the connection between technological innovation, ideological extremists and a weakened system of governance. This is one of those scenarios where the change of paradigm should be based on the abandonment of military-based approaches and the adoption of the governance-based approach, including human security, institutional legitimacy and resilience through participation (Bachmann & Gunneriusson, 2021). It is important to note that the term "hybrid warfare" itself is still contested and ill-defined; it is often used interchangeably with concepts such as "grey zone aggression". According to the securitisation literature, framing broad societal problems as existential threats can produce emergency politics that undermine democratic checks and deepen grievances (Buzan & Hansen, 2009).

Traditional interstate wars have declined and in their place the rise of advanced, hybrid wars in which one cannot draw a clear line between war and peace, combatants and civilians, physical and cyber spaces. Hybrid warfare is the intersection of conventional military tactics with non-traditional, cyber and informational techniques that attempt to undermine an enemy's cohesion and legitimacy. Therefore, hybrid threats reveal that the centre of gravity in modern conflict lies less in the battlefield and more in the political, informational and societal domains. Hybrid approaches changed our focus and mindset towards security threats by exploiting vulnerabilities in governance at the expense of a military strategy.

The Ukrainian, Syrian and Sahel wars illustrate the way hybrid conflict combines mainstream military assets with unconventional tactics, cyber-attacks and propaganda to destabilise regimes and demoralise the population. According to Galeotti (2016), Russia employed a combination of force, cyber activity, disinformation campaigns and covert political operations to achieve its objectives without provoking a full-scale war. Likewise, the US-China conflict is becoming increasingly hybrid, involving economic sanctions, advanced spying and cyber propaganda (Shambaugh, 2020). According to the recent evaluation by the RAND Corporation (2025), there is a strategic alignment of hybrid campaigns in both Russia and China to coordinate cyber espionage, disinformation and even maritime sabotage against democratic institutions across the globe. These are just some of the ways that hybrid warfare exploits the weaknesses of the governance system, the fragility of democracy and the lack of trust in the state apparatus among people.

The RAND Corporation (2021) states that it is much easier to resist hybrid coercion in States with high governance marked by transparency, institutional accountability and meaningful citizen participation. Brands and Porter (2020). This turns resilience in governance into a counter- and preventative strategy against hybrid insecurity. NATO and the EU also state that hard power cannot operate without resilience and governance (NATO, 2020; European Commission, 2020). The flawed counterargument, though, is that excessive dependence on such a wholes-of-society defence is manifested in the reappearance of such notions of total defence in Europe, which provokes the blurring of the boundary between civilians and non-combatants at the

cost of a tendentious annihilation of civil liberties and the inclusion of non-combatants into the battle zone. When citizens have faith in their institutions, they are less likely to be easily deceived by propaganda, corruption and foreign influence. Therefore, the legitimacy of governance is an element of psychological deterrence that works alongside military security.

According to a study conducted by the African Centre for the Study of Terrorism (ACSRT, 2022), in areas with weak governing institutions, there is the highest probability of a hybrid war. In such a case, isolated communities are denied political representation and social services, and this breeds resentment and becomes a soft target to be recruited by extremist groups and criminal networks. This perspective aligns with HST, which emphasises that insecurity occurs when people's freedom from fear, want, and indignity is at risk. Governance improvement through decentralisation, openness and people's participation has thus emerged as a top regional agenda. According to Kluijver (2025), Al-Shabaab has been taking advantage of governance incapacities by providing "simplistic justice" and taxation frameworks in areas or regions where the state or its machinery is absent, thereby gaining local legitimacy.

The conflict in Tigray underlined how hybrid war, through military activity in concert with cyber disinformation and humanitarian manipulation, endangers regional peace in Ethiopia. These cases first reveal the direct correlation between governance fragility and hybrid vulnerability. Hence, in the current times, governance capability has become an essential component of the national defence structure. Secondly, cyber and information warfare have become a significant component of hybrid insecurity, making the digital world a new war domain. Cyber-attacks against financial networks, election processes and official databases have increased globally. Rid and Buchanan (2015) argue that cyber operations have become the "fifth domain" of warfare, alongside land, sea, air and space. Thus, in contemporary times, governance capacity has emerged as an essential component of the country's defence establishment. Cyber threats further complicate the state/non-state dichotomy, with private hackers and cyber mercenaries being contracted out to fight proxy wars. For instance, the case of the 2016 U.S. election interference is the perfect example of how state and non-state actors use cyberspace to pursue disinformation operations and influence the opinion of people and erode democratic legitimacy. The United Nations Open-Ended Working Group on Cybersecurity (2021) noted that more than 70 countries have become victims of cyberattacks on their governance infrastructure, underscoring the magnitude of the new threat.

All these countermeasures are now likely to be governance-focused to counter cyber threats. In the 2020 Cybersecurity Strategy of the European Union, digital resilience supported by data protection, cyber diplomacy and multilateral cooperation is no less significant to security than military deterrence. The introduction of cybersecurity into the governance practices will help states to protect the safety of critical national infrastructure, digital rights, livelihoods and the dignity of their citizens. This action resonates with the concept of human security, which holds that the protection of the welfare, dignity and ability of all individuals to engage in the conduct of government at both the domestic and international levels is the cornerstone of international and local peace.

Hybrid Security Threats and Governance in Africa

The nexus between governance and security is a peculiarity on the African continent where a long-standing legacy of low state-building, asymmetric development and socio-political inequalities that are closely tied to hybrid threats on the continent. According to the Mo Ibrahim Index of African Governance (2022), approximately 70% of African countries have governance issues that directly affect insecurity. Governance instability breeds hybrid actors that include terrorist groups and insurgents, as well as transnational criminal syndicates. The Sahel is a good example. The process has only increased insurgency in Mali, Burkina Faso and Niger through military interventions. This phenomenon implies that the lack of appropriate governance institutions cultivates conducive grounds for the existence of hybrid actors. In a bid to fine-tune the examination of causal processes, this section uses the Opportunity, Motivation and Vulnerability (OMV) model.

Opportunity, Motivation and Vulnerability (OMV) Framework

Opportunity: The porous nature of the borders, with the help of corrupt officials, provides an easy target to operate and grow with the help of hybrid actors. An example is the propagation of the Al-Shabaab in the Somali border and all the way to Kenya because of the loose border and corruption, which makes it easy to pass individuals, weapons and illegal finances.

Motivation: A collection of sentiments, including grievance owing to political exclusion, joblessness and socioeconomic rejection, may cause individuals and factions to be estranged from participating in hybrid threats. The emergence of the IDCs of Boko Haram in West Africa and Al-Shabaab in the Horn of Africa evidences the establishment of local grievances with ideological militancy. However, it is also true that the IDC is associated with transnational organised crime (Onuoha & Thurston, 2019).

Vulnerability: When institutions of the communities are weak and low state legitimacy exists, the communities are most susceptible to being lured and recruited by hybrid actors; therefore, they are easily swayed. This insecurity is one example that has been perpetuated because of decades of political marginalisation, ineffective state institutions and underdevelopment in the Lake Chad Basin. The interplay of criminality, terrorism and failure of governance demonstrates that a hybrid threat cannot be restricted to military actions only. The lack of stability in the Sahel, then, demonstrates that guns without government can never result in long-term stability.

The International Crisis Group (2021) describes this persistence as stemming from the failure of governance, corruption and the marginalisation of peripheral groups. Although operations such as France's "Operation Barkhane" achieved tactical successes against insurgents, they could not bring about sustainable peace due to the absence of local governance transformation and inclusive development. There is limited academic consensus on how African states can bring together the reform of their governments and the transformation of their security sectors to achieve sustainable resilience. Both the African Peace and Security Architecture (APSA) and the African Governance Architecture (AGA) were designed to encompass conflict response that includes political, social and institutional dimensions. However, their operationalisation remains disparate and donor-driven, constraining their sustainability. African Union's (AU) Agenda 2063 aspiration 4 envisions a "Peaceful and secure Africa "built on democratic rule and respect for human rights (African Union Commission, 2015).

However, the policy-practice remains elusive, with the majority of states still investing in militarism over governance transformation. Such a policy practice disparages the spirit of human security and creates cycles of reactive rather than proactive security actions. Governance-based approaches have begun gaining momentum in Africa as a complementary measure to counterterrorism military actions. The African Union (AU) 2063 Agenda and the Silencing the Guns Initiative are both focused on people-centred governance, socio-economic development and conflict prevention through political negotiation (African Union, 2020). There are still implementation difficulties, especially in cases where high rewards, support networks and external forces sabotage local ownership of the peace process. Lines and Gebeye (2019) affirm that intergovernmental agencies, such as the Intergovernmental Authority on Development (IGAD), among others, have been registering remarkable progress in coordinating counterterrorism efforts. Nevertheless, institutional reforms that should include civilian checks, institutions of justice and economic participation are still required to make such endeavours sustainable.

Governance Deficits and Vulnerability to Hybrid Threats in Kenya

The gun-governance conversion is especially topical in the Kenyan case, where one might speak about a hybrid threat to security, as terrorism, radicalisation, cybercrime and transnational organised crime networks are the ones that are only gaining momentum. The Kenyan hybrid threat profile is similar to global and regional trends; hence, a strategic point of pursuing security based on governance. Kenya's closeness to Somalia and regional position in counter-insurgency have made it a front-line state and a potential target for retaliation and the most apparent one among them is Al-Shabaab. The most clear-cut examples of today's hybrid threat

environment are the 2013 Westgate Mall attack, the 2015 Garissa University attack and the latest attacks on Lamu and Mandera counties (Botha, 2014).

The Gen Z protests in Kenya in 2024 serve as a poignant example of how governance deficits create vulnerabilities within society. It is crucial to place this in context: although it is not a hybrid threat in and of itself, it represents a legitimate, digitally organised civic response to failures of governance, including corruption and political exclusion. Its decentralised nature, coupled with the use of social media, revealed how the state struggled to cope with digital-era discourse. Nonetheless, the securitisation response of the state was at first. The initial dependence by the state on the use of force by the police force, military force, mass arrests and recorded extrajudicial killings, however, was ineffective and only served to outrage the people and further legitimacy crises. The final move by the President of Kenya, Dr William Ruto, to switch the policy of confrontation to dialogue when the President invited youth representatives to the State House, is therefore the most appropriate way to emphasise the fact that governance engagement is the solution, rather than the military use of force, which is a long-term solution. The case illustrates the complex interplay between digital activism, state responses and the evolution of civic action in the digital age, highlighting the importance of nuanced and context-sensitive strategies for governance and security.

Previously, such use of force has failed in the counter-terror effort against Al-Shabaab in Kenya, where hard-power operations in Garissa, Mandera and Lamu have offered a reprieve but created local anger (Human Rights Watch, 2018). Similarly, police action in the 20072008 post-election violence and the most recent protests in 2017, resulted in additional fatalities without addressing the root causes of political and governance problems. These instances demonstrate that the hybrid security threats in Kenya, which evolve into radicalisation and civil strife, cannot be countered or reduced by force, but rather by governance reforms based on inclusivity, accountability, youth empowerment and women's empowerment. Conversely, the priority that Kenya has in investing in the military rather than community-based intelligence and socio-economic prevention models is a matter of dispute.

A good example of how a governance approach that prioritises community engagement, education and socio-economic empowerment as pillars of resilience should be followed is the NSCVE in Kenya, which was also established in 2016 (Republic of Kenya, 2016). Nevertheless, structural constraints, such as a lack of funds, political influence and the absence of indicators to measure its effectiveness, sabotage this process. The strategy will centre on local peace committees, religious figures and young people in detecting and preventing early signs of radicalisation. This participative and consultative approach demonstrates how the human security agenda focuses on giving individuals and communities a role as participants and beneficiaries of security. Additionally, the devolution structure of Kenya, as outlined in the 2010 Constitution, provides an institutional platform for decentralised administration and equitable resource allocation, which addresses some of the socio-economic imbalances that hybrid players exploit.

Though this is a provision in the Constitution, it is vitiated by corruption, absence of coordination and unequal distribution of resources. Despite this, the likelihood of such reforms having a functional effect is, however, constrained by the concerns of corruption, inefficiency in coordinating national government and counties, as well as insufficient investment into digital and intelligence infrastructure. The other emerging apprehensions in Kenya as a result of the hybrid security threat include cyber and environmental insecurity. The digitalisation of the financial platforms, public services and political communications has happened very rapidly and it has elevated the risks related to cyberattacks and disinformation campaigns to a level of importance.

According to the Communications Authority of Kenya (CAK, 2023), 400 million attempts were registered on the critical infrastructure of the country and databases of the most important institutions were compromised in 2022 alone. This points to the need to incorporate cybersecurity, data protection and digital literacy in national security planning. The vulnerability of the digital space highlights the importance of a governance-oriented solution that includes cybersecurity principles, data privacy laws and interagency cooperation. Equally, the existence of insecurities associated with climate-related factors, such as droughts, which may result in conflict and overuse of resources in arid regions, demonstrates that environmental pressures intensify the hybrid threats by increasing competition and causing the resettlement of weaker communities (Lind, 2020).

As such, the Kenyan hybrid threat environment is a multi-causal environment that involves a multi-sectoral approach.

In Kenya, effective governance to counter hybrid threats needs a comprehensive framework that does not focus just on state security. A whole-of-society approach must be the basis of this governance framework; it should be comprehensive, inclusive, legitimate, and accountable. For example, NCTC has been one of the crucial actors in the coordination of national efforts, but among differences like lack of trust in communities, respect for human rights, and not enough participation from the locals, as the case with (Human Rights Watch, 2018), still exist. The government can ease the social divide, which in turn can reduce the alienation, by officially involving local administration, the business sector, and civil society in security governance creating a well-established ownership. Besides, through investing in education reform, youth employment and inclusion, and digital literacy not only will the economy be more resilient but also the radical ideologies will offer less attractiveness, and the black markets which rely on poverty will be undermined as a result.

Ultimately, the Kenyan example demonstrates that hybrid threats are not only a security concern but also a governance issue. Therefore, when the Human Security Theory is incorporated as an analytical framework, it becomes clear that sustainable security should focus on the welfare of citizens, justice and participation rather than on coercion and force. The state will still be a major participant in defence and intelligence actions. However, it will be peace and resilience that are sustained by changing systems of governance to prioritise human security.

Table 2

The Critical Analysis of the Major Ideas of Kenyan Hybrid Security Discourse

Concept	**Analytical Strength**	**Operational Challenge**	**Manifestation in Kenya**
Governance-Centered Approach	Addresses root causes of instability	Difficult to measure impact; potentially slow to show results	NSCVE's community engagement is hampered by funding and political interference
Human Security Framework	Comprehensive; people-focused	Conceptually "fuzzy"; difficult to translate into policy	Tension between community welfare and immediate security demands in CT operations
Hybrid Threats	Captures the multidimensional nature of modern conflicts	Risk of overuse; may legitimate repression of legitimate dissent	The state's initial framing of Gen Z protests as security threats rather than political expression

Source: Researcher (2025)

The people-focused and government-focused strategies not only increase the security requirements but also enhance the long-term peace by providing solutions to the causes of insecurity. In this regard, the Kenyan experience can offer other African nations facing similar hybrid threats valuable lessons, namely that holistic designs are necessary to bridge the gap between development, governance and security.

Conclusion

This article explored the dynamic nature of hybrid security threats and assess the primary reason why governance, rather than military force, is the ultimate battleground for security resilience in the modern world. According to the global, regional and Kenyan examples, the paper revealed that hybrid threats prosper in environments that are characterised by weaker governance structures, accountability loss and civic participation deficits. In spite of the fact that the majority of the existing literature recognises the complexity of hybrid warfare, it is founded on the paradigm of state-centrism or militarisation. Within the framework of academic writing, this paper has shown that the issue of hybrid insecurity is one of governance, but not a military one and the discourses of securitisation tend to dominate, but not explain, too frequently.

The study disputes the existing beliefs within the literature regarding hybrid warfare in three different ways. To begin with, it helps to shift the balance of forces in favour of institutional validity by demonstrating that social trust, openness and active governance are more likely to predict resilience than military power. That position presents an apparent challenge to the prevailing wisdom that hybrid threats can be addressed solely through force-intensive, whole-of-government security architectures. Second, the analysis constructs an integrated Opportunity-Motivation-Vulnerability (OMV) framework that illustrates how hybrid actors exploit the absence of governance, rather than a lack of territorial or military strength, to facilitate exploitation and, in the process, enhances the conceptual tools used to understand the persistence of hybrid conflicts in Africa. Third, the Kenyan case provides an empirical foundation to refute the mainstream discourse that hybrid threats are driven solely by external opponents; this paper, instead, shows that internal failures in governance, youth marginalisation, corruption, cyber rights abuse and inequalities in devolution preconditions the entrenchment of hybrid insecurity.

By doing so, the study expands the literature on human security by demonstrating that human security should not merely be provided as a normative ideal, but also be practised as a working component of national defence. The Kenyan Gen Z unrest examined in this paper serves as a governance stress test, rather than a hybrid threat, further narrowing the arguments on digital age security. The over-securitisation of civic movements by the state would institutionalise more vulnerability, rather than diminishing risk. This understanding challenges the hybrid-threat discourse by demonstrating that a wrongful categorisation of a legal opposition as insecurity may, in turn, also be a hybrid vulnerability. The result of these findings is that it is impossible to have sustainable security, whether in Ukraine, the Sahel, or Kenya, based on guns without governance. The article is relevant to the academic discussion because it demonstrates that hybrid threats can be best defended when states adopt resilient digital governance, institutional reform and investments in socio-economic justice, civic trust and trust. In this case, the article narrows the theoretical connection between hybrid warfare and governance by presenting a more comprehensive and people-focused paradigm within which the concept of national security is integrated into the concept of human security. As African states work towards the targets of Agenda 2063 and the Silencing the Guns program of the African Union, this study proposes that the physical frontier is not the most significant battlefield in the future, but instead the legitimacy and ability of the state itself.

Recommendations

According to the analysis of global, regional and Kenyan case studies, the following recommendations are suggested first. They are based on the fundamental discovery that sustainable security necessitates uniting governance reforms with conventional security measures and are crafted with specific implementation tracks and stakeholders in mind.

Create a multi-agency security team that integrates military solutions with governance solutions and socio-economic solutions to address hybrid threats, such as terrorism, transnational organised crime and cyber insecurity. This involves the incorporation of cyber resilience, digital literacy and cooperation among intelligence agencies across countries.

Rebalance the approaches of national security; Kenya and other African states should institutionalise a paradigm of governance reforms to be given priority in national security, which include transparency, inclusion and accountability. It can be achieved by incorporating governance indicators into national security measurements, as well as implementing systems of performance-based accountability within security agencies.

Enhance local governance and devolution as initial components of hybrid-threat resilience: Hybrid threats thrive in areas where governance vacuities exist, so building stronger counties is at the heart of prevention. Such a strategy can be reached through offering more funding to counties to support youth programs, digital literacy and community policing activities.

Design a national digital resilience architecture: Kenya should assume cyberspace as a governable space due to the scale of cyberattacks and digital disinformation experienced in the country. For this reason, the government should bring on board a unified, multi-agency team that links NIS, CAK, the private sector and county ICT departments.

Strengthening the National Strategy to Counter Violent Extremism: The article mentions NSCVE as an under-funded yet effective governance instrument. The Kenyan government needs to develop a monitoring and evaluation framework with a clear outcome matrix while providing adequate and ring-fenced financing for county CVE action plans.

Develop a national framework for managing digital era protests and civic movements: The Gen Z protests have highlighted the dangers of misclassifying civic action as security threats. The National Security Council should draft protocols for lawful policing of digitally coordinated protests. Some of the protocols ought to involve retraining police on digital rights, online assembly and nonviolent crowd management. Civic dialogue platforms should also be integrated into national early-warning mechanisms.

Address socio-economic drivers of hybrid vulnerability: Since the study has identified poverty, unemployment and exclusion as the primary sources of both motivation and vulnerability, the government should expand targeted youth employment schemes in borderland and marginalised regions, as well as increase investment in dryland economies to reduce resource-conflict pressures. Cross-border markets and legal trade corridors should also be introduced and encouraged to disincentivise illicit networks.

References

African Centre for the Study and Research on Terrorism (ACSRT). (2022). *Mid-Year Africa Terrorism Trend Analysis 2022.* Algiers: African Union. https://archives.au.int/handle/123456789/10353.

African Union Commission. (2015). *Agenda 2063: The Africa we want.* Addis Ababa: African Union.

African Union. (2020). *Silencing the Guns in Africa by 2030: An Implementation Roadmap.* Addis Ababa: African Union.

Aning, K., & Atta-Asamoah, A. (2011). *Managing threats of terrorism in Africa: Building effective regional and national counterterrorism frameworks* (ISS Monograph Series No. 181). Pretoria: Institute for Security Studies.

Bachmann, S. D., & Gunneriusson, H. (2021). Hybrid warfare and hybrid threats: The new (old) normal? *Journal on Baltic Security, 7*(1), 7–20. https://doi.org/10.2478/jbs-2021-0002

Botha, A. (2014). Radicalisation to terrorism in Kenya and Uganda: How Al-Shabaab recruits and identifies its targets (*ISS Paper 265*). Pretoria: Institute for Security Studies.

Brands, H., & Porter, P. (2020). *Resilience and deterrence in the age of hybrid threats.* RAND Corporation. https://www.rand.org.

Buzan & Hansen (2009) and Williams (2020) are authoritative sources for military/force modernisation, as well as traditional security studies.

Cascio, J. (2020, April 29). Facing the age of chaos. Medium. https://medium.com/@cascio/facing-the-age-of-chaos-b00687b1f51d

Clapham, C. (2021). *The Horn of Africa: State formation and decay.* Oxford: Oxford University Press.

Communications Authority of Kenya. (2023). *Cybersecurity report 2022.* Nairobi: CAK. https://ca.go.ke/reports.

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade.* Brussels: European Union.

European Commission. (2020, December). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient*. Press release.

European External Action Service. (2020, December). *Towards a More Secure, Global and Open Cyberspace: The EU Presents Its New Cybersecurity Strategy*. EEAS. European External Action Service.

Galeotti, M. (2016). Hybrid, ambiguous and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies, 27*(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170.

Gonçalves, C. P. (2020). Cyberspace and artificial intelligence: The new face of cyber-enhanced hybrid threats. In *Cyberspace.* London: IntechOpen. https://doi.org/10.5772/intechopen.91908.

Hoffman, F. (2007). *Conflict in the 21st century: The rise of hybrid wars.* Arlington, VA: Potomac Institute for Policy Studies.

Human Rights Watch. (2018). *Kenya: Counterterrorism operations undermine rights.* New York: HRW. https://www.hrw.org.

International Crisis Group. (2021). *A course correction for the Sahel stabilisation strategy* (Africa Report No. 299). Brussels: ICG. https://www.crisisgroup.org.

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

Kluijver, R. (2025, September 25). *Al-Shabab's shadow state: Why Somalia's militants are winning legitimacy*. The New Humanitarian. https://www.thenewhumanitarian.org/analysis/2025/09/25/al-shabab-why-somalia-militants-winning-legitimacy*15*(3).

Lind, J. (2020). Adaptation, resilience and conflict: Climate change and insecurity in Kenya. *Political Geography, 82*, 102238. https://doi.org/10.1016/j.polgeo.2020.102238.

Luckham, R., & Kirk, T. (2013). Understanding security in the vernacular in hybrid political contexts: A critical survey. *Conflict, Security & Development, 13*(3), 339–359

MacFarlane, N., & Khong, Y. (2006). *Human security and the UN: A critical history*. Indiana University Press.

Mo Ibrahim Foundation. (2022). *The Ibrahim Index of African Governance (IIAG) 2022 Report.* London: Mo Ibrahim Foundation.

NATO. (2020). *Countering Hybrid Threats: NATO's Approach* Brussels: North Atlantic Treaty Organisation. https://www.nato.int.

Newman, E. (2010). *Critical human security studies*. Review of International Studies, 36(1), 77–94.

Nowell, L., Norris, J., White, D., & Moules, N. (2017). Thematic Analysis. *International Journal of Qualitative Methods*, 16. https://doi.org/10.1177/1609406917733847.

Omeje, K. (2013). *Youth unemployment and violent extremism in Africa*. Journal of African Peace and Security, 5(2), 15–32.

Onuoha, F. C., & Thurston, A. (2019). The Rise of Boko Haram and the Governance Challenge in West Africa. *Journal of Contemporary African Studies, 37*(2), 147–162. https://doi.org/10.1080/02589001.2019.1614788.

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security, 26*(2), 87–102. https://doi.org/10.1162/016228801753191141.

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, 26(2), 87–102.

Renz, B., & Smith, H. (2016). Russia and hybrid warfare: Going beyond the label. *Aleksanteri Papers 1/2016.* University of Helsinki.

Republic of Kenya. (2016). *National Strategy to Counter Violent Extremism (NSCVE).* Nairobi: Ministry of Interior and Coordination of National Government.

Rid, T., & Buchanan, B. (2015). Attributing cyberattacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382.

Rotberg, R. I. (2004). *When states fail: Causes and consequences.* Princeton University Press**.**

Sarjito, A. (2024). Countering hybrid threats: Challenges and the role of defence science. *PUBLICNESS: Journal of Public Administration Studies, 3*(1), 101–111. https://doi.org/10.24036/publicness.v3i1.188.

Shambaugh, D. (2020). *Where great powers meet: America and China in Southeast Asia.* Oxford: Oxford University Press.

Stewart, F. (2008). *Horizontal inequalities and conflict: Understanding group violence in multi-ethnic societies*. Palgrave Macmillan.

Tadjbakhsh, S., & Chenoy, A. M. (2007). *Human security: Concepts and implications.* London: Routledge.

United Nations Development Programme (UNDP). (1994). *Human Development Report 1994: New dimensions of human security.* New York: Oxford University Press.

United Nations Open-Ended Working Group on Cybersecurity. (2021). *Report on developments in the field of information and telecommunications in the context of international security.* New York: United Nations.

Williams, P. D. (2020). *Security studies: An introduction (3rd ed.). Routledge.*

Williams, P. D., D'Alessandro, M., Darkwa, L., de Coning, C., Helal, A., Machakaire, J., & Rupesinghe, N. (2018, December 16). *Assessing the effectiveness of the African Union Mission in Somalia (AMISOM).* Effectiveness of Peace Operations Network (EPON) / Norwegian Institute of International Affairs (NUPI). https://nupi.brage.unit.no/nupi-xmlui/handle/11250/2597243