

Impact of Intelligence Gathering, Coordination, and Technological Capabilities on the Effectiveness of Security Forces in Asymmetric Conflict Scenarios

Odongo Michael Onyango¹, Ngari Lazarus Kinyua²

Department of Security, Diplomacy and Peace Studies, Kenyatta University

DOI: <https://doi.org/10.47772/IJRISS.2026.100800679>

Received: 17 August 2026; Accepted: 22 August 2026; Published: 15 September 2026

ABSTRACT

This study examined the impact of intelligence gathering, coordination, and technological capabilities on the effectiveness of security forces in asymmetric conflict scenarios. The study was anchored on two complementary theories namely; Just War Theory and Irregular Warfare Theory. The study adopted a descriptive research design. The target population comprised KDF personnel, NPS officers, Private Security officers, Security Policy Experts, and Local Administrators. This study employed stratified purposive sampling technique to identify the various categories of respondents. A total of 65 study participants were selected for field interviews. The research instrument used were interview guides, structured questionnaires and documentary analysis. Qualitative data from interviews and open-ended questions underwent thematic content analysis and was presented narratively to provide detailed perspectives from security personnel. Quantitative data was analyzed using descriptive and inferential statistics and presented in tables and graphs. The study found that effective intelligence gathering, inter-agency coordination, and technological capabilities significantly enhance security forces' preparedness, situational awareness, response speed, and operational effectiveness. The study recommends integrated intelligence systems, advanced surveillance technologies, permanent joint command centres, regular inter-agency exercises, predictive analytics, secure communication networks, and continuous personnel training to strengthen Kenya's response to asymmetric threats.

Keywords: Intelligence Gathering; Inter-Agency Coordination; Technological Capabilities; Security Forces; Asymmetric Warfare.

Background to the Study

The global security landscape is becoming more and more dominated by conflicts that include non-state entities, thus forcing security units to address challenges that can be different from traditional warfare (Grosu, 2023; Rubbi et al., 2020). Asymmetric warfare is a great departure from conventional warfare and has to do with the fact that weaker participants tend to exploit weaker points of stronger participants with the help of irregular and unconventional tactics (Mkuti, van Wyk, & Tella, 2024; Smith, 2020). Such tactics can be represented in guerrilla operations, raids, sabotage, terrorism, improvised explosive devices (IEDs), psychological operations, as well as the exploitation of civilian population and poorly governed borders. Due to this, the effectiveness of the security forces is becoming more and more connected not only with their military power but also with their ability to gather and process intelligence, synchronize their actions across units, and apply appropriate technologies.

Different sources reveal how important the role of intelligence and ability to adapt is in the fight against asymmetric threats. For example, Smith (2020) mentions that the Quds Force was more effective when the socio-political climate was supportive and also when it managed to apply nontraditional methods, and an effective tactic of being dynamic – using covert operations. Treiblmaier (2023) states that terrorist groups use their decentralized structures to penetrate the vulnerabilities of the victim countries and blend into civil society, which complicates the military response. According to Riggs (2021), in Iraq and Afghanistan, those tactical responses that have a narrow focus are usually ineffective when dealing with adaptive enemies and consume enormous

resources. Similarly, Mkuti, van Wyk, and Tella (2024) found out that technological superiority does not guarantee success in the Middle East conflicts.

The situations in Africa illustrate the importance of intelligence gathering and inter-agency cooperation, as well as the need for technology. Ambushes, sabotage, and assassinations were techniques used by Anglophone separatists in Cameroon that put conventional military actions to the test (Ekah, 2022). The flexible nature of Boko Haram's operations in Nigeria restricted the applicability of traditional military tactics (Okoli & Lenshie, 2022). In Somalia, Al-Shabaab has exploited cross-border operations as well as unconventional methods in order to induce the state reactions and exacerbate social divisions (Ibrahim Shire, 2023).

Kenya is experiencing similar issues relating especially to Al-Shabaab terrorist activities and other threats to its security posed by neighboring countries. Problems of border insecurity encompass smuggling, cattle rustling, organized crime, ethnic conflict, and rivalry over resources (Gito & Rono, 2018; Shidane, 2020). The Kenyan Defense Forces (KDF) operations in Somalia face a major challenge from the use of IEDs, which are low-cost, hard to detect, and versatile in terms of application (Ibrahim Shire, 2023; Lusiola, 2021). While Kenya has taken steps to improve cooperation in the region, establish defense diplomacy and carry out joint trainings, coordination issues as well as limited funds and competing development priorities can undermine the effectiveness of these efforts (Lusiola, 2021; Nyamao, 2021; Riggs, 2021).

Thus, asymmetric threats are evolving, making it vital for the security services to employ intelligence-led, coordinated, and technical measures in their approach. Multinational cooperation and training has improved the capabilities of the region to respond to such threats. Nevertheless, the continued occurrence of asymmetric attacks shows the need to assess if present-day intelligence systems, coordination mechanisms, and technical capabilities suffice to solve the problem at hand. This research focuses on how intelligence-gathering, coordination, and technical systems affect the performance of the security services when dealing with asymmetric threats. Understanding this issue is crucial for improving operability, decision-making, inter-agency cooperation, and developing the required training and operational systems.

Statement of the Problem

Kenya is facing asymmetric security threats from terrorist groups like Al-Shabaab. The threats are more pronounced where attacks happened using guerrilla tactics, and improvised explosive devices (IEDs) in civilian areas (National Counter Terrorism Centre, 2022). The number of attacks increased from 34 in 2019 to 69 in 2020, and there were 122 deaths and 42 injuries reported (Centre for Human Rights and Policy Studies, 2021; Centre for Human Rights and Policy Studies, 2022). There was a reduction in attacks to 51 in 2021, but the death toll was still at 100 and 73 people suffered injuries during the attacks. These recent developments indicate that there are serious challenges facing security agencies in Kenya despite the declined number of attacks. A number of factors make tackling asymmetric threats difficult, with lack of coordination and technological adoption and limited intelligence contributing to ineffectiveness of responses.

Despite substantial investment in national security, agencies continue to encounter operational difficulties arising from porous borders, limited intelligence resources, and the socio-political complexities of border areas, particularly along the Kenya-Somalia frontier (National Counter Terrorism Centre, 2022). Effective responses to asymmetric conflict therefore require timely intelligence gathering, effective coordination among security agencies, and appropriate technological capabilities to support surveillance, threat detection, information sharing, and operational decision-making.

Existing studies have examined civil-military cooperation, defence diplomacy, and borderland security (Nyamao, 2021; Kaberere, 2021; Muteti, Giotto, & Rono, 2018), but limited empirical attention has been given to how intelligence gathering, inter-agency coordination, and technological capabilities influence the effectiveness of Kenyan security forces in asymmetric conflict scenarios. This study addressed this gap by examining the impact of intelligence gathering, coordination, and technological capabilities on the effectiveness of security forces in asymmetric conflict scenarios in Kenya, providing evidence to inform policy, resource allocation, operational planning, and security preparedness.

Purpose of the Study

To examine the impact of intelligence gathering, coordination, and technological capabilities on the effectiveness of security forces in asymmetric conflict scenarios.

LITERATURE REVIEW

Asymmetric warfare is defined as a type of armed conflict where there is a big difference in the capacities of the fighting sides, where the weaker side is able to exploit the weaknesses of the stronger side by means of different forms of unconventional warfare (Chehtman, 2022). Unconventional means include the use of guerrilla warfare, terror acts, ambush, various sabotage acts, IEDs, cyber warfare, and psychological warfare, and all these forms of warfare allow not state actors to avoid direct fighting and achieve the impact that is disproportionate in the social and psychological terms (Hameed, Rahman & Khanam, 2022; Rubbi et al., 2020). This means that asymmetric warfare has already crossed the borders between such notions as war and peace, combatants and civilians, and international and domestic security (Chehtman, 2020).

According to Dakour (2022), Amarasinghe (2023), and Abonyi (2023), conventional conflict and asymmetric warfare create legal and humanitarian challenges, especially when non-state players and technology are involved. However, their studies concentrate mainly on international humanitarian law, and there is little consideration of Kenyan security forces in terms of operation. Likewise, in writing on asymmetric warfare, authors Hameed, Rahman, and Khanam (2022) point out how asymmetrical warfare results in complex non-linear ramifications and Rubbi et al. (2020) demonstrate how technological capabilities, including cyber, space, and missile technologies, can change the understanding of conventional military weaknesses.

The practical difficulties of asymmetric warfare have been highlighted by studies carried out in Africa. Ekah (2022) reported that the separatist fighters in Cameroon rely on ambushes, sabotage, kidnappings and assassinations, thus making a traditional military approach impractical. Mharapara et al (2014) underline the psychological and ideological aspects of asymmetric warfare as a conflict. Ibrahim Shire (2023) shows how Al Shabaab is using guerrilla warfare to provoke an excessive reaction from the state and break up societal cohesion. In the study conducted by Mkuti et al (2024), it was shown that asymmetric partnerships are capable of enhancing the capacity of countering terrorism. Therefore, what these scholars show in their research work is that asymmetric warfare the ability of an armed force to employ not only military superiority, but intelligence, coordination, flexibility and technology.

The nature of asymmetric warfare means changes in the way training and operations are conducted by security forces. Chehtman (2022) and Grosu (2023) argue that normal tactics are not enough to deal with versatile and dispersed enemy forces and therefore there must be the emergence of counterinsurgency capacities, intelligence, quick-response technology-based capabilities. Grosu stresses flexible doctrine, technological advancement, international cooperation and capacity for interoperability.

Riggs (2021) found that costly tactical actions against asymmetric threats in Iraq and Afghanistan did not create significant strategic effects. Thus, according to this, security forces should choose to focus on intelligence-led and system approaches instead of relying only on costly technology. Nevertheless, Rodriguez (2022) shows that military operations may influence the organizations, procedures, technologies and cultures required for adaptation that highlights the importance of experience gained during the process of operations. Aina (2023) agrees that the Special Operations Forces of Nigeria are able to learn and gain from trainings, skills and equipment although too much reliance on elite units may have a negative impact on their effectiveness.

In Kenya, Muteti, Giotto and Rono (2018) established that border insecurity is facilitated by inadequate resources, corruption and weak inter-agency collaboration. The study recommended improved training, joint patrols and intelligence sharing. Kabereere (2021) found that civil-military cooperation in Lamu improved information sharing and relations between security forces and communities. Africa Defense Forum (2022) further demonstrated the value of multinational exercises in Kenya and Rwanda, particularly in developing

interoperability, urban combat capabilities, medical response, communication and coordination among military, police and civilian actors.

Security forces face significant challenges because asymmetric actors exploit weaknesses in conventional security systems through low-cost and adaptable tactics such as IEDs, ambushes, terrorism and cyber operations (Rubbi et al., 2020). Their integration into civilian populations complicates intelligence gathering and increases the risk of civilian casualties (Ekah, 2022). Cross-border threats further complicate operations because states may have different political interests, legal frameworks and operational capabilities (Mkuti, van Wyk, & Tella, 2024).

Nuciari and Olivetta (2021) found that military leaders operating in asymmetric environments require flexibility, cultural awareness and strong relational skills. Treiblmajer (2023) similarly argues that decentralized terrorist networks operating within civilian communities create legal and operational difficulties. Smith (2020) demonstrates that successful irregular warfare depends on social and political conditions, specialized tactics, intelligence and flexible covert strategies. Okoli and Lenshie (2022) found that Nigeria's conventional counterinsurgency strategies were insufficient against Boko Haram, recommending integrated military and non-military approaches.

Regional collaboration can create issues. Lusiola (2021) stated that competing interests of the respective countries, insufficient resources and weaknesses of the institution impacted AMISOM's work. Nyamao (2021) reported that there were challenges related to policies, resources and coordination in Africa's defense diplomacy as well. Furthermore, Shidane (2020) noted that insecurity in the Kenya-Ethiopia border is aggravated by ethnic conflicts, competition over resources, lack of personnel, corruption and absence of coordination. All these studies confirm that coordination, intelligence and technology matter when coping with asymmetric threats.

Despite the existence of studies on asymmetric warfare, the training of troops, border security, intelligence sharing, interoperability and technology components, there are scanty empirical research on how intelligence collection with the help of coordination between several agencies and technology influence the performance of Kenyan security forces in asymmetric warfare situation.

Similarly, Grosu (2023), Riggs (2021), Rubbi et al. (2020) and Africa Defense Forum (2022) emphasize technology and interoperability without specifically examining their combined influence within Kenya's security environment. This study therefore addresses the empirical and contextual gap by examining the impact of intelligence gathering, coordination, and technological capabilities on the effectiveness of security forces in asymmetric conflict scenarios in Kenya.

THEORETICAL FRAMEWORK

This study was anchored on two complementary theories namely; the Just War Theory and the Irregular Warfare Theory to explain a holistic approach to the ethical as well as the operational nature of the asymmetric warfare. The choice of these theories was based on the fact that they are in direct correspondence with and contribute to all three research objectives. Collectively, these theories offered a solid theoretical basis on the study of the manner in which security forces can adequately and ethically react to asymmetric warfare challenges and revise their training and operation strategies.

RESEARCH METHODOLOGY

This study employed a descriptive research design using a mixed approach. The descriptive nature of the design enabled in-depth recording of operation experiences, training requirements, and security force adaptation whereas the cross-sectional design enabled efficient data gathering of various agencies of security and geographical regions.

The target population comprised KDF personnel, NPS officers, Private Security officers, Security Policy Experts, and Local Administrators from the North-Eastern Region, Coastal Region, and Kenya-Somalia border

areas. Sampling. This study employed stratified purposive sampling technique to identify the various categories of respondents. A total of 65 study participants were selected for field interviews. The research instrument used were interview guides, structured questionnaires and documentary analysis. Qualitative data from interviews and open-ended questions underwent thematic content analysis and was presented narratively to provide detailed perspectives from security personnel. Quantitative data was analyzed using descriptive and inferential statistics and presented in tables and graphs. Respondents were distributed as follows;

	Category of Informant	Sampled	%
1	KDF Personnel	25	38.5%
2	NPS Officers	25	38.5%
3	Private Security Officers	5	7.7%
4	Security Policy Experts	5	7.7%
5	Local Administrators	5	7.7%
	Total	65	100%

Analysis, Interpretation and Presentation of Findings

Response Rate

Table 1.2 Response Rate

	Category	Sampled	Responded	Not Responded	Response Rate
1.	KDF Personnel	25	23	2	92%
2.	NPS Officers	25	22	3	88%
3.	Private Security Officers	5	5	0	100%
4.	Security Policy Experts	5	5	0	100%
5.	Local Administrators	5	5	0	100%
	Total	65	60	5	92.3%

The response rate in this study was 92.3%. In terms of categories, Private Security Officers (PSOs), Security Policy Experts and Local Administrators had a 100% response rate, thus showing full participation of these key stakeholder groups. The response rate for Kenya Defense Forces (KDF) personnel was 92%, with 2 non-responses and for National Police Service (NPS) Officers, 88% with 3 non-responses. There were a few variations, but all categories had satisfactory participation in the survey, meaning that the results are representative and do not lack a range of security viewpoints.

The Impact of Intelligence Gathering, Coordination, and Technological Capabilities on the Effectiveness of Security Forces in Asymmetric Conflict Scenarios

Table 1.3 Impact of intelligence gathering

Impact of intelligence gathering	SA	A	NS	SD	D	MS	SD
Effective intelligence gathering	2948.3%	2033.3%	46.7%	35.0%	46.7%	1.55	1.03
Limited technological capacity	2643.3%	2236.7%	58.3%	35.0%	46.7%	1.62	1.07
Real-time intelligence sharing	3050.0%	1830.0%	58.3%	35.0%	46.7%	1.55	1.09
Modern surveillance technologies,	2745.0%	2135.0%	46.7%	46.7%	46.7%	1.62	1.11
Poor inter-agency coordination	2541.7%	2440.0%	35.0%	46.7%	46.7%	1.63	1.06
Joint training and collaboration strengthen	2846.7%	2033.3%	58.3%	35.0%	46.7%	1.58	1.05

The research findings reveal that intelligence gathering, technological capability, and inter-agency coordination play a crucial role in enhancing the security forces' capability to combat asymmetric threats in Kenya. Most respondents (48.3% strongly agree, 33.3% agree) agreed that good collection contributes to good operations. This highlights the importance of timely and accurate intelligence and actionable information for tactical and strategic decision-making, enabling forces to proactively anticipate threats, deploy assets effectively, and make informed decisions.

The technological capacity was also emphasized as a factor that influences the operation. 43.3% strongly agreed and 36.7% agreed that limited technological capability has a negative impact on operational effectiveness and 80% agreed that the modern technologies of counter-terrorism (such as drones, communication monitoring systems etc.) enhance counter-terrorism operations. Such results indicate that the technological differences limit the real-time monitoring, the swift identification of threats, and the dissemination of data, which decreases the responsiveness of the operation in asymmetric conflict situations.

Real-time intelligence sharing" came as a top concern when it comes to the success of the mission, with 50% stridently agreeing and 30% agreeing. The data show that when the information flows efficiently among the agencies, they are more likely to be coordinated while minimizing duplication and ensuring operational decisions are made with the latest intelligence. 81.7% of the respondents (41.7% strongly agree, 40% agree) also noted that "Poor coordination" was a factor leading to delayed responses, reflecting the drawbacks of poor communication and organizational silos.

Collaboration and joint training were also highly supported (46.7% strongly agree; 33.3% agree) as ways of improving operational effectiveness. These results point to the need for a common skillset, harmonization of procedures, and trust between agencies to ensure best use of resources and tactical operations.

The results indicate that intelligence capability, technology tool and collaborative coordination are coupled factors which have significant influence on operational performance. African security forces must be better trained, equipped with modern technology, and have an institutional mechanism in place for inter-agency coordination, if they are to respond, operate and be effective against asymmetric threats.

The majority of the interviewees agreed that intelligence gathering is a main component of success in an asymmetric conflict. Asymmetric threats are extremely fluid and unpredictable, unlike traditional military threats that have a pattern of force deployment and can often be anticipated well in advance, so intelligence is a central element of anticipatory planning and immediate response. Human intelligence (HUMINT) from the local community, signals intelligence (SIGINT), and surveillance information are all being used to monitor militant movements, potential target locations, and to disrupt potential planning operations before they become a threat, according to security officers.

Notwithstanding its importance, respondent identified some issues that impact the effectiveness of the security forces in intelligence operations. Limited resources, inadequate training and limited technological tools are the first reason and reduce the accuracy and comprehensiveness of information gathered, which hinders intelligence collection. Some respondents reported challenges in reaching outpost and/or high-risk remote locations where militant groups operate, creating a lack of situational awareness. Moreover, the analysis and interpretation of intelligence in a timely fashion is limited due to the lack of qualified analysts and standard procedures for validation and the dissemination of intelligence.

Security personnel also noted that the coordination of information from various sources such as community informants, technical surveillance and inter-agency reports is not always good, leading to gaps or inconsistencies that impact on operational planning. Respondents also commented on the difficulty in operationalizing intelligence without causing civilian casualties, and the need for care in acting on sensitive information in order to prevent collateral damage. These findings suggest that mere collection is not sufficient to intelligence effectiveness; there must be effective intelligence analysis and coordination systems and fast decision-making systems.

Inter-agency coordination has always been regarded as one of the main elements of operational success. Asymmetrical threats may cross borders and require collaboration between military, police and intelligence and civilian agencies. Effective coordination means sharing common operational picture, fast flow of intelligence and coordinated actions commitment to joint operational planning and activities such as joint planning meetings, establishment of common headquarters, and conducting joint patrols.

Respondents also pointed out to the existence of some problematic aspects, namely bureaucracy delays, lack of coordination between agencies, and competing trust levels among them that interferes with promptness and coherence of actions at the operational level. According to the findings, with respect to the above-mentioned challenges the agencies with the better level of inter-agency coordination, have the capability to react to sudden attacks and avoid escalation of the conflict, and poor coordination results in failures in security coverage or effectiveness of operation. Overall, inter-agency coordination is a key aspect of operational success.

The role of technology in enhancing the capabilities of operations was emphasized. Respondents indicated that drones, remote sensing devices, and real-time monitoring technologies enable the security forces to monitor areas of hostility without putting people at direct risk. Talk-throughs are established via secured radio systems and mobile command post offices to enable quick coordination and decision-making among elements and agencies. Others noted the importance of software for data analysis that would allow for the analysis of surveillance and signals intelligence data, thereby helping to predict the movements of militants and to identify potential threats early on. In addition, technology will improve logistical planning by monitoring the movement of personnel, equipment and supplies during operations. There were also limitations, such as training to keep employees up to speed on the complex systems, maintenance and high cost, acknowledged by respondents. Despite such limitations, there was a general agreement that technology significantly increases situational awareness, precision, speed of response to asymmetric threats and minimizes casualties and operational risk.

Respondents shared some illustrative examples of how intelligence, coordination and technology can be critical. One of these was when, in a northern border area, intelligence gathered from local contacts helped to anticipate an attack by the insurgents. Operating in a combined manner between the military, police and intelligence, the security forces could intercept the insurgents before they entered into civilian areas that would result in casualties and damage. Another example pointed to the use of drones and remote surveillance in urban operations, which enabled real-time information about the enemy, allowing units to make targeted interventions, while reducing any risk to civilians.

Study participants made recommendations about how to enhance intelligence, coordination and technology. This included investing in sophisticated information-gathering tools, ensure more training of the analysts and create regular ways of intelligence collection, validation and communication. Respondents pointed out that mandates should be clear, and training should be conducted jointly, and permanent communication structures should be established to ensure well-coordinated actions and to gain trust, good decision-making and to lessen delays in the coordination process. The technological advice suggested was to use more drones, predictive analytics, reliable means of real-time communications, continuous maintenance, and training of the operators. Respondents also mentioned the necessity to establish integrated command centres that could help consolidate intelligence, planning, and operational management in order to boost quick reaction capacity.

The findings provide insight that in asymmetric conflict, intelligence, inter-agency coordination, and technology are key factors in determining overall effectiveness of operations. While intelligence offers the foresight that is needed for anticipatory planning, intelligence has limitations and is hampered by constraints on resources, gaps in analysis and difficulties operationalizing intelligence. Agency coordination improves situation awareness and operational coherence, but can be hampered by bureaucracy and agency roles. The integration of technological systems like drones, surveillance systems, and secure communications networks greatly improves the accuracy of operations, mobility, and risk management. The examples below prove that a mix of these factors can make a difference, with failure in one of them being able to make all the difference in mission success or failure. Respondents call for investments to continue in intelligence infrastructure, advanced technology and institutional structures for coordination for effective responses to asymmetric threats.

The findings of this study show that intelligence, inter-agency coordination and technology play a vital role in the effectiveness of the Kenyan Security Forces in asymmetric warfare. The respondents highlighted the dynamism, diffuseness and uncertainty of asymmetric threats, which require intelligence-led operations. This is consistent with the scholarship on intelligence which outlines how intelligence is the backbone of modern counter-insurgency operations and counter-terrorism activities (Kalyvas, 2006; Kilcullen, 2009). Asymmetric warfare differs from traditional warfare in that it lacks the structure of the battlefield and relies on guerrilla and other warfare methods, improvised explosive devices and surprise attacks. The Kenyan experience, as described by the respondents, reinforces the fact that intelligence is a vital input for situational awareness, quick deployment and strategic planning in an urban/rural setting. These results echo those of Metz and Johnson (2001), who claim that in theatres of irregular warfare, timely and actionable intelligence is a key factor in ensuring the success of operations.

The focus on human intelligence (HUMINT), signals intelligence (SIGINT), and surveillance highlights the nature of modern intelligence operations which are based on multiple sources. The respondents noted the importance of HUMINT sourced through local communities to gain insight into militant networks, safe havens and planned operations. This is consistent with other literature that indicates that human intelligence is essential for counter-insurgency, especially when the application of technological monitoring is limited or ineffective (Hoffman, 2006; Kilcullen, 2009). Moreover, SIGINT and real-time surveillance data can be utilized to improve predictive and operational planning, helping to allocate military resources efficiently and reduce unnecessary exposure to risk. The findings corroborate the findings by studies conducted in East African counter-terrorism settings where it has been noted that human intelligence and technical intelligence have the best mix of countering asymmetric threats (Odhiambo, 2018; Gatluak, 2015).

Some respondents noted that intelligence was crucial, and they continually cited operational struggles that hinder its effectiveness. Limited resources, inadequate training and training tools, and limited use of more advanced information-gathering tools result in poor quality and timeliness of information collected. These findings are in line with intelligence studies conducted on security forces in Africa, which frequently showed that limited resources, lack of analysts training and technology gaps often affect the effectiveness of intelligence (Peters, 2008; Odhiambo, 2018). In addition, problems with remote or high-risk areas and with getting all the information in one place represent what Biddle (2006) and Møller (2013) find, that information silos and lack of inter-agency cooperation can undermine operational planning in irregular warfare. Respondents' issues of operationalizing intelligence whilst minimizing civilian harm are consistent with the wider literature, which highlights population-centric approaches, and where information has to be acted upon carefully to ensure it retains legitimacy and prevents backlash (U.S. Army Field Manual 3-24, 2006; Kilcullen, 2009).

The results have also shown the need of coordination between the agencies in order to increase the operational effectiveness. Respondents highlighted the need for effective inter-agency cooperation and coordination (military, police, intelligence, and civilian agencies) to allow for shared situational awareness, timely information sharing, and coordinated responses. These findings corroborate those of Kilcullen (2009) and Hoffman (2006) who highlighted that asymmetric threats can often cross multiple jurisdictions and thus need coordinated multi-agency responses. Positive examples have been cited, such as joint planning meetings, mobile command centers, and coordinated patrols, which are representative of the general impression of the benefits of integrated operations in reaching a greater operational range and eliminating duplication of effort (Kiras, 2006; Metz & Johnson, 2001).

Respondents, however, also reported ongoing issues with inter-agency coordination, such as delays in bureaucracy, overlapping mandates and lack of trust. These limitations are also described in the literature on African security institutions, which observes that often the hierarchical nature of police institutions, political interference, and a lack of clarity regarding operational authority (Branch & Mampilly, 2005; Peters, 2008) impede joint operations. The balance between collaboration and institutional friction can cause delays, gaps in operations, and even mission failure. Based on these findings, it is clear that mandates and joint training need to be established, as well as institutionalized communication channels, in line with current counter-terrorism studies (Metz & Johnson, 2001; Kilcullen, 2009).

Feedback from survey participants shows that technology is instrumental in today's asymmetric warfare. Technology, such as drones, remote sensing, real-time surveillance, and secure communications networks improves situational awareness, precision, and agility in operations. Real-time signals intelligence (SIGINT), data analysis, and predictive analysis help create informed decisions and identify possible attackers. The studies on African counter-terrorism also indicate that the integration of technology is crucial in achieving missions since armies with limited numbers would be able to defeat hidden and flexible enemies (Biddle, 2006; Echevarria, 2005; Odhiambo, 2018; Gatluak, 2015).

The respondents' awareness of the technological constraints such as expenses, maintenance and a need for special training also aligns with previous studies. Technological adoption doesn't just involve initial technological purchase, but also includes ongoing maintenance along with training of operators and integration with operational planning (Kilcullen, 2009; Hoffman, 2006). The results show that technology improves the ability to operate, but it requires appropriate resourcing, institutional support, and ongoing staff training.

Respondent quotations of illustrative examples further highlight the interdependency of intelligence, coordination, and technology in influencing outcomes. Elements such as preemptive interception of insurgents, coordinated joint responses and operations using drones to help in urban operations, all collectively contribute to increasing the chances of success of the operation and reducing the number of civilians getting harmed. On the other hand, failures in any area (intelligence, coordination, or technology) can affect the effectiveness of the mission. The findings in these cases support larger-scale evidence in the literature that successful operations in an asymmetric conflict depend on the effective integration of human, technological and institutional capabilities (Kalyvas, 2006; Kilcullen, 2009).

Lastly, respondents suggested the measures to be taken for intelligence gathering, coordination and technological systems. Recommendations such as the need for investment in advanced surveillance tools, analyst training, standardizing intelligence procedures and the creation of integrated command centers mirror best practice identified in the African and international counter-insurgency literature (Metz & Johnson, 2001; Biddle, 2006). The focus on institutionalized inter-agency cooperation, regular training and investment in technology is a testament to a growing body of contemporary research that a successful, sustainable operational effectiveness is possible only in the context of asymmetrical situations, where tactical skill is only one part of the equation, as organizations and technology play an equally important role.

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

The study notes the key role of intelligence gathering, inter-agency coordination and technology in the effectiveness of Kenyan security forces in asymmetric conflict scenarios. Anticipatory planning, prioritization of resources and real-time decision making, based on both human intelligence, signals data and surveillance. But it's constrained by limited resources and training, gaps in analysis, issues with implementing sensitive information and other limitations. Close relationship between agencies yielding shared situational awareness, coordinated response, and efficient operations is the best outcome of inter-agency coordination, while lack of coordination through bureaucratic delays, overlapping mandates and lack of trust can lead to ineffectiveness.

Technological solutions such as drones, remote sensing, real-time monitoring, and secure communication networks improve monitoring, mobility, precision and risk management which are challenges that need to be addressed. Illustrative cases demonstrate that gaps in any of these three domains can lead to the failure of prevention and mitigation efforts; gaps in intelligence, coordination and technology can lead to a failure in one or all. Participants suggest continued efforts in developing and investing in advanced surveillance systems, predictive analytics, operator training and exercises, and integrated command centers to facilitate decision making and operations oversight. The results, overall, highlight the need for a multifaceted approach through a mix of human, technological and institutional aspects to enhance Kenya's preparedness, responsiveness and effectiveness in combating the asymmetric threats.

This study recommends the adoption of an inclusive model should be entrenched that combines intelligence collection, cutting-edge technological systems (including drones, predictive analytics, and safe communications

network), and institutional cooperation. The setting up of permanent joint command centers, regular inter-agency exercises and continuous training of personnel on intelligence analysis and technological operations will improve situational awareness, speed of response and precision of operations.

REFERENCES

1. Abonyi, A. U. (2023). An assessment of the nature, scope and responses towards addressing the scourge of asymmetric warfare. *Chukwuemeka Odumegwu Ojukwu University Journal of Commercial and Property Law*, 4(1), 80–96.
2. Africa Defense Forum. (2022). East African troops train for peacekeeping missions at Exercise Justified Accord. U.S. Africa Command.
3. Aina, F. (2023). “Phantom operators”: Special operations forces and asymmetric warfare in Northern Nigeria. *Defence Studies*, 23(2), 177–197. <https://doi.org/10.1080/14702436.2023.2206958>
4. Amarasinghe, K. (2023). Applicability of international humanitarian law in asymmetric warfare: A review on Sri Lankan civil war. SSRN. <https://doi.org/10.2139/ssrn.4394908>
5. Biddle, S. (2006). *Military power: Explaining victory and defeat in modern battle*. Princeton University Press.
6. Branch, A., & Mampilly, Z. C. (2005). Winning the war, but losing the peace? The dilemma of SPLM/A civil administration and the tasks ahead. *The Journal of Modern African Studies*, 43(1), 1–20.
7. Centre for Human Rights and Policy Studies. (2021). Trends of violent extremist attacks and arrests in Kenya, January–December 2020 (Report No. 4).
8. Centre for Human Rights and Policy Studies. (2022). Trends of violent extremist attacks and arrests in Kenya, January–December 2021 (Report No. 5).
9. Chehtman, A. (2022). Asymmetrical warfare. In O. P. Richmond & G. Visoka (Eds.), *The Palgrave encyclopedia of peace and conflict studies*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-77954-2_27
10. Dakour Al Aridi, A. (2022). The problem of hybrid war in international law [Doctoral dissertation, Vilnius University]. <https://doi.org/10.15388/vu.thesis.401>
11. Echevarria, A. J., II. (2005). *Fourth-generation war and other myths*. Strategic Studies Institute, U.S. Army War College.
12. Ekah, E. R. (2022). Asymmetric warfare in contemporary Africa: The case of the Anglophone secessionist struggle in Cameroon. *Global Journal of Human-Social Science: H—Interdisciplinary*, 22(6), 7–21.
13. Grosu, R. (2024). An academic approach of the military doctrine transformation in the context of asymmetrical conflicts. *Strategic Impact*, 90(1), 23–50. <https://doi.org/10.53477/1842-9904-24-2>
14. Hameed, M. A., Rahman, M. M., & Khanam, R. (2022). Assessing the asymmetric war-growth nexus: A case of Afghanistan. *PLOS ONE*, 17(8), e0272670. <https://doi.org/10.1371/journal.pone.0272670>
15. Hoffman, B. (2006). *Inside terrorism* (Rev. & expanded ed.). Columbia University Press.
16. Ibrahim Shire, M. (2023). Provoking an overreaction: Transborder guerrilla warfare in the Kenya-Somalia borderlands. *African Security*, 16(1), 61–94. <https://doi.org/10.1080/19392206.2023.2192641>
17. Johnson, D. V., & Metz, S. (2001). Asymmetry and U.S. military strategy: Definition, background, and strategic concepts. Strategic Studies Institute, U.S. Army War College.
18. Kaberere, A. M., & Mulu, F. (2022). Civil military cooperation (CIMIC) as a strategy for security stabilization operations: Case of Lamu County, Kenya. *International Journal of Scientific and Research Publications*, 12(5). <https://doi.org/10.29322/IJSRP.12.05.2022.p12561>
19. Kalyvas, S. N. (2006). *The logic of violence in civil war*. Cambridge University Press.
20. Kilcullen, D. (2009). *The accidental guerrilla: Fighting small wars in the midst of a big one*. Oxford University Press.
21. Kiras, J. D. (2006). *Special operations and strategy: From World War II to the war on terrorism*. Routledge.
22. López-Rodríguez, G. (2022). Building military expeditionary culture: Spanish Army after international operations. *Defense & Security Analysis*, 38(4), 410–430. <https://doi.org/10.1080/14751798.2022.2114582>

23. Mharapara, R., Bangidza, L. B., & Gwekwerere, S. (2014). Asymmetric warfare: Experiences, perspectives, inkling and challenges with a focus on Zimbabwe. *Austral: Brazilian Journal of Strategy & International Relations*, 3(5), 97–115.
24. Mkuti, S., Van Wyk, J.-A., & Tella, O. (2024). United States–Kenyan asymmetry in counterterrorism cooperation: An assessment of the efforts of the United States and Kenya in East Africa. *Scientia Militaria: South African Journal of Military Studies*, 52(1), 87–122. <https://doi.org/10.5787/52-1-1448>
25. Møller, J. (2013). When one might not see the wood for the trees: The ‘historical turn’ in democratization studies, critical junctures, and cross-case comparisons. *Democratization*, 20(4), 693–715. <https://doi.org/10.1080/13510347.2012.659023>
26. Muteti, S. M., Gioto, V. A., & Rono, J. K. (2018). Borderland-related crimes and security threats in Kenya (NCRC Research Report No. 13). National Crime Research Centre.
27. Nuciari, M., & Olivetta, E. (Eds.). (2021). *Leaders for tomorrow: Challenges for military leadership in the age of asymmetric warfare*. Springer. <https://doi.org/10.1007/978-3-030-71714-8>
28. Nyamao, E. M. O. (2021). The role of defence diplomacy in enhancing regional stability in Africa: Case study of Kenya Defence Forces [Master's research project, University of Nairobi]. University of Nairobi Repository.
29. Odhiambo, N. A., Ochara, N. M., & Kadymatimba, A. (2018). Structuring of the terrorism problem in the digital age: A systems perspective. In 2018 Open Innovations Conference (pp. 148–154). IEEE. <https://doi.org/10.1109/OI.2018.8535619>
30. Okoli, A. C., & Lenshie, N. E. (2022). “Beyond military might”: Boko Haram and the asymmetries of counter-insurgency in Nigeria. *The Security Journal*, 35(3), 676–693. <https://doi.org/10.1057/s41284-021-00295-1>
31. Riggs, D. (2021). Re-thinking the strategic approach to asymmetrical warfare. *Military Strategy Magazine*, 7(3), 40–48. <https://doi.org/10.64148/msm.v7i3.6>
32. Rubbi, L. N., Álvarez Magañini, V., Nascimento, L., & Sager, D. (2020). Asymmetric warfare: Exploratory study on the non-conventional military developments of the People’s Republic of China in the period 2012–2018. *Revista SAAP*, 14(1), 181–200. <https://doi.org/10.46468/rsaap.14.1.N3>
33. Shidane, J. M. (2020). The cross-border security challenges in the Horn of Africa region: A case study of Kenya, Ethiopia Moyale border [Master's thesis, University of Nairobi]. University of Nairobi Repository.
34. Smith, C. B. (2020). The Quds Force model: What makes irregular warfare effective in asymmetric conflict [Master's thesis, Naval Postgraduate School]. Calhoun: Institutional Archive of the Naval Postgraduate School.
35. Treiblmaier, A. (2021). The new wars: Terrorism and “asymmetric” warfare. *Vojenské rozhledy*, 30(4), 93–108. <https://doi.org/10.3849/2336-2995.30.2021.04.093-108>.